COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, AND INTELLIGENCE (C4I) INTEROPERABILITY: ARE WE THERE YET?

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

BRIAN J. WORTH, MAJOR, USAF
B.S., University of Maryland, European Division, 1994
M.A., Webster University, St. Louis, Missouri, 1994

Fort Leavenworth, Kansas
2008

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
13-06-2008	Master's Thesis	AUG 2007 – JUN 2008

4. TITLE AND SUBTITLE
Command, Control, Communications, Computer, and Intelligence (C4I) Systems Interoperability: Are We There Yet?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

WORTH, Brian J., Major, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This study examines command, control, communications, computer, and intelligence (C4I) systems interoperability progress within the United States (U.S.) military services and amongst coalition partners since the year 2000. This study uses national military strategy, joint military strategy, service unique strategy and doctrine, Joint Tactical Radio System (JTRS) and Defense Integrated Military Human Resource System (DIMHRS) case studies, Defense Information Systems Agency (DISA) technological standards, C4I technical reports to establish trends, patterns, and gaps in coalition interoperability. C4I interoperability successes are abundant since 2000 but it is clear from current day operations and research that the U.S., its allies and coalition partners need further improvements in order to master the many moving parts required for true coalition C4I systems interoperability. Clearly, acquisition, development, testing, and fielding must be fully integrated into either a joint or coalition solution.

In order to achieve C4I interoperability, this study recommends changes in law, namely to the Goldwater-Nichols Act of 1986 to further define the strategic intent of system interoperability among services of the DoD and foreign nations. Changes to national military strategy, joint military strategy, and service-unique military strategy are required to overhaul and emphasize the unequivocal need for fully interoperable C4I systems across the DoD and amongst coalition members. Acquisition, although not fully explored within this study, requires a greater emphasis in order to speed delivery of these interoperable systems to the field. Development and testing mechanisms exist throughout industry and within the military services to ensure interoperability but again, speed requires greater emphasis to ensure the technological advancements meet the soldier, sailor, airman, and marine before they become obsolete. Demands will likely increase tenfold over the next decade given the complexity and lethality of current and next generation weapons systems, so C4I interoperability costs will likely rise also. Budgets must accurately reflect this expense and place national-level interest on this vitally important national and international domain.

Training, operations and maintenance expenditures related to C4I across the services rise annually at exorbitant rates as authorized manpower shrinks and contractor support skyrockets. Efficiencies through standardization of training, joint operations and exercises, and common maintenance practices within DoD can yield substantial savings and concentrate efforts along similar planes. These efforts, along with a concerted C4I interoperability life cycle system, can yield the necessary interoperability to ensure warfighters of the future have at their disposal the most integrated, efficient, and lethal means of conducting military affairs.

15. SUBJECT TERMS
command, control, communications, computer, and intelligence, C4I Interoperability, Joint Tactical Radio System, JTRS, Defense Integrated Military Human Resource System, DIMHRS, Defense Information Systems Agency, DISA,

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	90	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE
THESIS APPROVAL PAGE

Name of Candidate: Major Brian J. Worth

Thesis Title: Command, Control, Communications, Computer, and Intelligence (C4I) Systems Interoperability: Are We There Yet?

Approved by:

_____, Thesis Committee Chair
Lieutenant Colonel John B. Esch, M.M.A.S.

_____, Member
Alexander M. Bielakowski, Ph.D.

_____, Member
Lieutenant Colonel John D. Rye, M. S.

Accepted this 13th day of June 2008 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

COMMAND, CONTROL, COMMUNICATIONS, COMPUTER, AND INTELLIGENCE (C4I) SYSTEMS INTEROPERABILITY: ARE WE THERE YET? by Major Brian J. Worth, 90 pages

This study examines command, control, communications, computer, and intelligence (C4I) systems interoperability progress within the United States (U.S.) military services and amongst coalition partners since the year 2000. This study uses national military strategy, joint military strategy, service unique strategy and doctrine, Joint Tactical Radio System (JTRS) and Defense Integrated Military Human Resource System (DIMHRS) case studies, Defense Information Systems Agency (DISA) technological standards, C4I technical reports to establish trends, patterns, and gaps in coalition interoperability. C4I interoperability successes are abundant since 2000 but it is clear from current day operations and research that the U.S., its allies and coalition partners need further improvements in order to master the many moving parts required for true coalition C4I systems interoperability. Clearly, acquisition, development, testing, and fielding must be fully integrated into either a joint or coalition solution.

In order to achieve C4I interoperability, this study recommends changes in law, namely to the Goldwater-Nichols Act of 1986 to further define the strategic intent of system interoperability among services of the DoD and foreign nations. Changes to national military strategy, joint military strategy, and service-unique military strategy are required to overhaul and emphasize the unequivocal need for fully interoperable C4I systems across the DoD and amongst coalition members. Acquisition, although not fully explored within this study, requires a greater emphasis in order to speed delivery of these interoperable systems to the field. Development and testing mechanisms exist throughout industry and within the military services to ensure interoperability but again, speed requires greater emphasis to ensure the technological advancements meet the soldier, sailor, airman, and marine before they become obsolete. Demands will likely increase tenfold over the next decade given the complexity and lethality of current and next generation weapons systems, so C4I interoperability costs will likely rise also. Budgets must accurately reflect this expense and place national-level interest on this vitally important national and international domain.

Training, operations and maintenance expenditures related to C4I across the services rise annually at exorbitant rates as authorized manpower shrinks and contractor support skyrockets. Efficiencies through standardization of training, joint operations and exercises, and common maintenance practices within DoD can yield substantial savings and concentrate efforts along similar planes. These efforts, along with a concerted C4I interoperability life cycle system, can yield the necessary interoperability to ensure warfighters of the future have at their disposal the most integrated, efficient, and lethal means of conducting military affairs.

ACKNOWLEDGMENTS

I would like to thank my wife Linda Worth who encouraged me throughout the research, writing, and editing of this thesis. I would like to thank my parents for their kind support as I bounced ideas off them as well.

I wish to acknowledge the support, assistance, and guidance of my thesis committee: Lt Col John Esch, Dr. Alexander Bielakowski, and Lt Col J. D. Rye. My thesis committee supported me throughout the entire process and offered candid opinions, which always kept me focused and on track.

I also wish to acknowledge the outstanding service of the CARL Library Staff. This library is probably the best in DOD as far as I am concerned. On a number of occasions they went far beyond my expectations by providing top-notch research assistance. I could not have completed this without their devoted help.

Finally I wish to thank the CGSC Graduate Degree Program Office, especially Ms. Elizabeth Brown and Dr. Robert Baumann. The staff provided excellent groundwork from which to begin work and made the process easier to understand and follow. They always had time to listen.

TABLE OF CONTENTS

Page

ACRONYMS

ADPO	Army's DIMHRS Program Office
C2	Command and Control
C4I	Command, Control, Communications, Computers, and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAOC	Combined Air Operations Center
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CSTB	Computer Science Telecommunications Board
DCGS	Distributed Common Ground-Surface System
DIMHRS	Defense Integrated Military Human Resources System
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDD	Department of Defense Directive
FCS	Future Combat System
GAO	Government Accounting Office (
GCCS	Global Command and Control System
GCCS-J	Global Command and Control System Joint
GIG	Global Information Grid
IA	Information Assurance
ICD	Initial Capabilities Document
IT	Information Technology
JCIDS	Joint Capabilities and Integration Development System
JCS/J6	Joint Chief of Staff, Command, Control, Communications Office

JEFX	Joint Expeditionary Force Experiment
JIEO	Joint Interoperability Engineering Organization
JITC	Joint Interoperability Test Command
JPEO	Joint Program Executive Officer
JTA	Joint Technical Architecture
JTRS	Joint Tactical Radio System
JWID	Joint Warfare Interoperability Demonstration
MCTFS	Marine Corps Total Force System
NDS	National Defense Strategy
NMS	National Military Strategy
NRR-KP	Net-Ready Key Performance Parameters
NSS	National Security System
ORD	Operational Requirements Document
PM	Program Manager
POM	Program Objective Memorandum
QDRR	Quadrennial Defense Review Report
TEW	Terrorist Early Warning
U.S.	United States

ILLUSTRATIONS

Page

TABLES

Page

CHAPTER 1
INTRODUCTION

> Interoperable, high-volume communications systems are essential to conducting operations across a dispersed command space. Our systems operate near full capacity daily with little surge capability. Because many of our needs must be satisfied by commercial providers, access to them is critical. The largest challenge we face is integration of disparate systems into interoperable and reliable networks. We must embrace policies that enable successful integration and technologies that result in effective interoperability and efficient information-sharing.
>
> Admiral William J. Fallon
> C205, Reading E

Introduction

The Goldwater-Nichols Act of 1986 established the legal need for joint operations between services and drove command, control, communications, computers, and intelligence (C4I) technology to dramatically change and shape the joint operating environment. Although some argue the United States (U.S.) is a long way from full C4I joint operations, the information age ushered in a plethora of new interdependent computer systems and capabilities that did not exist when this legislation was passed over twenty years ago. It may be time to revisit the progress to date and examine efficiencies that can be gained in terms of C4I. Each armed service developed its own C4I technologies throughout its existence, resulting in "stove-piped" or service-unique systems. As a result of legislation, these stove-piped C4I systems have since become interoperable with other services systems to eliminate duplication and confusion on the battlefield. Research should reveal the progress to date and possibly layout courses of action for fully integrated and interoperable C4I systems across the armed services.

Background and Context

C4I interoperability is grounded in the Goldwater-Nichols Reorganization Act of 1986 and further illustrated within the *National Defense Strategy (NDS) of the United States of America*, dated March 2005. A review of strategy, objectives, and tasks associated with C4I interoperability from the national level down to the service level should serve as a good beginning point for determining progress on a scale of accomplishment.

The *NDS* stresses the importance of C4I interoperability when it states: "Operations in the war on terrorism have demonstrated the advantages of timely and accurate information, while at the same time reinforcing the need for even greater joint, interoperable command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR)" (Department of Defense 2005b, 14). It goes on to point out expected returns on this investment: "Beyond battlefield applications, a network-centric force can increase efficiency and effectiveness across defense operations, intelligence functions, and business processes by giving all users access to the latest, most relevant, most accurate information. It also enables 'reach-back' by more effectively employing people and capabilities without deploying them forward" (Department of Defense 2005b, 14). There is clearly linkage from law to the Department of Defense's (DoD) interpretation of the importance of C4I interoperability documented within the DoD strategy.

The NDS feeds the next level of strategy titled *The National Military Strategy (NMS) of the United States of America* and is signed by the Chairman of the Joint Chiefs of Staff as the senior military advisor to the Secretary of Defense and President of the

United States. The *NMS* further delineates U.S. resolve to sharpen its C4I spear by stating, “Dynamic decision-making brings together organizations, planning processes, technical systems and commensurate authorities that support informed decisions. Such decisions require networked command and control capabilities and a tailored common operating picture of the battle space. Networking must also provide increased transparency in multinational operations and support the integration of other government agencies and multinational partners into joint operations. Force application, sustainment and actions to secure battle space will rely on these capabilities” (Chairman, Joint Chiefs of Staff 2004, 20). This answers the question, “what” but leaves open the question of “how” as one would expect in a strategy document.

The *NMS* attempts to answer “how” this is possible by providing the following roadmap, “The DOD is further developing a fully interoperable, interagency-wide global information grid (GIG). The GIG has the potential to be the single most important enabler of information and decision superiority. The GIG supports the creation of a collaborative information environment that facilitates overlapping operations. It will be a globally interconnected, end-to-end set of information capabilities and associated processes. These activities are among the ongoing efforts related to improving information sharing among coalition partners” (Chairman, Joint Chiefs of Staff 2004, 25). So, potential courses of action to solve any C4I interoperability dilemma, now and in the future, will likely be closely linked to the development and implementation of the GIG in an effort to achieve net-centricity (Department of Defense 2006, 58). To evaluate progress to date in C4I interoperability, a glimpse into the *Quadrennial Defense Review Report* (*QDRR*) of 2006 is in order.

One of the core purposes of the *QDRR* in 2006 was to assess the "need for considerably better fusion of intelligence and operations to produce action plans that can be executed in real time" by defining a "shift in emphasis" from "service and agency intelligence--to truly Joint Information Operations Centers," which capitalize on C4I interoperability of systems across joint and coalition forces since the start of the Global War on Terrorism in 2001 (Department of Defense 2006, vi). What the *QDRR* found was evidence of the need to emphasize the importance of C4I interoperability at the highest levels of national government within the DoD and interagencies. "As an enterprise asset, the collection and dissemination of information should be managed by portfolios of capabilities that cut across legacy stove-piped systems. These capability portfolios would include network based command and control, communications on the move and information fusion. Current evolving threats highlight the need to design, operate and defend the network to ensure continuity of joint operations" (Department of Defense 2006, 58). This acknowledgement of the gap in C4I interoperability is paramount to any future successes the U.S. may attain in the joint and coalition war fighting environments.

The DoD efforts to integrate joint operations under the C4I umbrella have yielded dramatically new ways of doing business, like net centric warfare and the Joint Tactical Radio System (JTRS). The technological revolution that has taken place since 1986 significantly changed the face and complexity of war by opening up new dimensions unheard of before the year 2000. Although the services leaned forward to develop, implement, and refine their own C4I systems, duplication still exists between those systems and the service departments. Some feel the lack of an overarching architectural strategy for the DoD is the root impediment to true interoperability, while others view the

attempt frugal due to the complexity of system software code and network architecture. It is time to review the law, strategy, objectives, and tasks associated with C4I interoperability and ascertain if the U.S. military has made sufficient progress. This study may discover opportunities for more efficient operations, training, and maintenance within the services under the C4I umbrella.

Research Questions

Some of the questions that need to be answered during this review are: "What do U.S. military services need to achieve C4I interoperability in an effort to streamline operations?" Secondary questions are: "What life cycle planning tools exist to ensure C4I interoperability in the DoD and joint environment?" and "Is C4I interoperability a plausible schema for future joint and coalition operations?"

Assumptions

These questions require a few assumptions to limit the scope of any research effort. First assumption is that C4I is a sanctioned term by the national leadership and will continue to be paramount to any future war. The second assumption is C4I spans five dimensions: air, space, land, sea, and cyberspace. Lastly, C4I does not have boundaries within one or more of the military services necessary for any level of war. C4I interoperability challenges exist in every domain and are not specifically tied to one particular service or country.

Limitations

Because C4I encompasses all dimensions of war and contains five elements (command, control, communications, computers and intelligence), it may be difficult to

capture a true picture of interoperability progress across all services. Due to the complexity and scope of the proposed research area, an acknowledged constraint is the time available to adequately answer the thesis questions. C4I interoperability significantly impacts joint and coalition operations. Given the condensed research time for this thesis some aspects may not be thoroughly covered due to the time constraints. The focus of improving C4I interoperability will tend toward larger systems with broader impact to military wartime operations. Two case studies were reviewed to demonstrate C4I interoperability progress in real time.

Delimitations

A core foundation for this research is based upon a previous Masters of Military Art and Science (MMAS) thesis completed by Major Michael B. Black, USAF, titled, "Coalition Command, Control, Communications, Computer, and Intelligence Systems Interoperability: A Necessity or Wishful Thinking?" dated 2000. Research in C4I interoperability within this work will begin where Black left off in order to determine progress to date and to limit the scope of this thesis. Other theses from various military institutions involving C4I interdependence and interoperability may be cited for relevance to the research subject, but the research window for this thesis begins from the year 2000 to present day.

Significance of the Study

This study is important to the communications and information career fields within the Air Force, signal corps of the Marine Corps, Army, and Navy as it discussed C4I interoperability as it exists today and what it will look like in the future. Some

experts link this discussion directly with how the uniformed services should be organized or reorganized, as the case may be, based upon the information flow to expedite getting the intelligence to the warfighter in the fastest manner possible. "In the future, C4I collection assets could consist of micro-air vehicles, micro robots, and motes ("smart dust") capable of travelling through air, land, and space providing direct inputs to the Soldiers fighting enemies in irregular wars" (Martinage 2007). In this instance, the system of systems becomes even more important so the applicability of this subject is not limited to communications professionals but anyone involved in joint or coalition operations or wars. The goal of this paper is to assess and report progress in C4I interoperability in the DoD, its allies, and coalition members.

CHAPTER 2
CURRENT STATE OF C4I INTEROPERABILITY

Introduction

The Joint Interoperability Test Command (JITC) at Fort Huachuca, Arizona, tests systems to determine whether they will be truly interoperable once fielded to the services. They are the C4I interoperability certification testing executive agent for the Joint Forces Command and stand as the final litmus test on systems prior to production. As the keystone to interoperability, JITC participates in joint exercises and routinely identifies shortfalls in capabilities. Oddly enough, some JITC customers overlook the shortfalls to maintain their stove-piped systems that "work well."

JITC is testing the Global Command and Control System Joint (GCCS-J) and once it passes the "GCCS-J will be the single C4I system to support the warfighter from the foxhole to the command post" (JITC 2008, 1). GCCS-J will fuse together forty-two separate C4I systems through an interoperable software environment, which illustrates the complexity of C4I interoperability as it exists in the military environment today. JITC tests and evaluates system architecture through modeling and simulation tools to ensure the interfaces between systems, as in GCCS-J system, work properly and information flows seamlessly. Complex as this seems, it is absolutely necessary for the warfighter in the field who depends upon timely and accurate information from all sources.

In his statement to the Senate Armed Services Subcommittee On Terrorism, Unconventional Threats And Capabilities, Lieutenant General William S. Wallace, Commanding General, Combined Arms Center, U.S. Army Training And Doctrine Command, clearly articulated the need for a concerted effort to embrace C4I

interoperability requirements as it was having a direct effect on soldiers in Iraq (House Armed Service Committee 2003). C4I interoperability is integral to winning wars on land, in the air, on the seas, and in cyberspace. Future wars will depend upon dominance in the C4I arena.

Admiral William Fallon, in like fashion, stressed the importance of C4I interoperability when he said, "interoperable, high-volume communications systems are essential to conducting operations across a dispersed command space. Our systems operate near full capacity daily with little surge capability. Because many of our needs must be satisfied by commercial providers, access to them is critical. The largest challenge we face is integration of disparate systems into interoperable and reliable networks. We must embrace policies that enable successful integration and technologies that result in effective interoperability and efficient information-sharing" (C205RE, 21). Admiral Fallon clearly identified the need to emphasize interoperability in future C4I systems while also addressing the existing limitations and increasing demands placed upon information superiority during wartime.

Black researched C4I interoperability in 2001 while attending the Command and General Staff College in a thesis titled, "Coalition Command, Control, Communications, Computer, and Intelligence Systems Interoperability: A Necessity or Wishful Thinking?" He evaluated C4I interoperability progress within the confines of the joint perspective and coalition environment and summarized his research conclusions by saying, "It is clear from previous operations and past research that the US, allies, and coalition partners have not mastered coalition C4I systems interoperability" (Black 2000, iii). Black's thesis set a foundation for assessing C4I interoperability beginning from the year 2000 to

the present day. He assimilated the research conducted within the DoD military schools of thought at the time and provided a core understanding of what constituted C4I interoperability as well as what could potentially improve allied and coalition interoperability. "As operations become truly coalition in nature, where countries are bringing their own equipment to the fight, it is apparent that C4I system interoperability is a must to properly command and control forces" (Black 2000, 23). Black's research is used as a reference point for the beginning of this thesis and is referenced several times throughout this study.

A study commissioned by the Defense Authorization Act of 1996 and detailed in the 1999 book titled, *Realizing the Potential of C4I, Fundamental Challenges* was not included in Black's reference list or body of research. This book constitutes a comprehensive look at the services attempt at inter- and intra-service interoperability as well as doctrinal reviews of architectures and costs associated with interoperability integration. This study was engineered and assembled by the Computer Science Telecommunications Board (CSTB) of the National Research Council by putting together a team of notable experts during this era in C4I. There are many lessons learned that still apply today and these will be brought to the surface and revealed as either applicable or not to this study. The core mission of the CSTB team is identified below.

> The Defense Authorization Act for Fiscal Year 1996 requested the National Research Council undertake a review of current and planned service and defense-wide programs for command, control, communications, computers and intelligence (C4I) with a special focus on cross-service and inter-service issues. Programs for C4I account for some of the most complex systems, technologies, and functions in the military. Expenditures on C4I represent a significant fraction of the defense budget. C4I programs provide an interrelated group of capabilities that are distributed horizontally across the military services and vertically within each defense function. (National Academy of Science 1999, viii)

Albeit dated, the information contained within this C4I study assembles strategic thought around the keys to effectively managing C4I interoperability within the DoD and provides a core framework for enhancing expenditures, research, capability, and industry efforts. This study will further amplify the direction of interoperability across the services and help identify current gaps and trends discussed in detail in chapter 3.

Although this study is limited to the service departments of the DoD, there are civilian C4I interoperability challenges, which surfaced following the terrorist attacks of 9/11 on the Twin Towers and these efforts could reveal potential military solutions. One example of particular note is the Terrorist Early Warning (TEW) model first established in Los Angeles County in 1996 (Bunker 2003, 150). As described by the author, the TEW "follows a networked approach, integrating law enforcement, fire, health, and emergency management agencies to address intelligence needs for terrorism and critical infrastructure protection. The TEW integrates local-federal echelons and operates pre-, trans-, and post-incident" (Bunker 2003, 151). The Los Angeles TEW possesses a backbone of service personnel interoperating through a common infrastructure of communications toward the common goal of deterring terrorism.

This system or "model," as Bunker refers to it, is very much like the C4I systems within the DoD as it operates to provide a common operating picture for all agencies. "The TEW essentially provides two functions: indications and warning, and operational net assessment. To do so, it is evolving the next generation of command, control, communication, computers, intelligence, surveillance, and reconnaissance (C4ISR) tools and seeking to identify ways to bridge interdisciplinary gaps and build appropriate mechanisms for civil-military interoperability" (Bunker 2003, 151). Interestingly

enough, the TEW model seeks to integrate all known factors surrounding a terrorist threat, assimilate the data and information from the various agencies and then produce courses of action for dealing with the threats. Casting the net beyond the DoD pool for solutions to any discovered C4I interoperability shortfalls may prove beneficial in support of this study as indicated in the Los Angeles TEW description above.

Several existing DoD funded programs under execution are in various levels of completion with the ultimate goal of providing a joint, cross-service, and in many cases cross-national military capability to replace existing stove-piped C4 systems. A short survey of some of these existing programs and systems will paint the picture for how well C4 interoperability is being induced within the DoD community and world at large. This system survey will seek to define the C4ISR certification process as it relates to life cycle management. Once the process is defined, then a glimpse at two existing, joint programs, JTRS and Defense Integrated Military Human Resources System (DIMHRS), will paint a clearer picture of interoperability progress in real time. These case studies will provide insight into programs that have been on the books for years and yet stand incomplete due to C4I interoperability shortfalls and may also provide indications as to whether interoperability is technically and feasibly viable in today's world. How does a system, program, project, piece of equipment become "certified" as C4I interoperable?

C4I interoperability rules and procedures are spelled out in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01D, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*. The purpose of this instruction, as applicable to all service departments within the DoD, is to "assure that

DoD components develop, acquire, and deploy Information Technology (IT) and National Security Systems (NSS) that:

1. Meet the essential operational needs of US forces.
2. Are interoperable with existing and proposed IT and NSS.
3. Are supportable over the existing and planned Global Information Grid.
4. Are interoperable with allies and coalition partners.
5. Are net-ready.
6. Allow US forces to protect mission essential data.
7. Detect and respond to network intrusion/system compromise.
8. Restore mission essential data. (CJCSI 6212.01 2006, 3)

Although this is a broad statement of purpose, the instruction defines specifically who it is applicable to as Joint Staff, services, combatant commands, defense agencies, and joint and combined activities. This essentially encompasses all elements of the DoD to include interagencies as well. The important focus of this instruction is on interoperability and is further defined and refined in the ensuing 144 pages of specific process instructions. So how is it possible to meet the spirit and intent of a system to become C4I interoperable?

The answer to that question is extremely loaded because in many cases meeting the requirements to become C4I interoperable within DoD or with coalition partners is nearly impossible or impractical. The Joint Chiefs of Staff J6 (JCS/J6) office, Director of Command, Control, Communications, and Computer (C4) Systems, is the lead agency overseeing the various processes, which monitor, evaluate, and approve C4I interoperability. Accordingly, the J6 provides the current assessment of C4I

interoperability on a public website and "approximately 25-28 percent of IT/NSS systems are interoperability certified" (JCS/J6 2006, 1). The paper goes on to specify how systems may complete interoperability certification or not if the system in question will no longer be in use five years from now. Essentially, any system, which touches the GIG must have interoperability documentation on file with J6 and the various levels of certification muscled through JITC or seek waivers to this requirement. The paper also implies that if a system lacks money to complete the interoperability requirements, it may apply for a waiver until such time the system is funded to meet these stringent interoperability requirements.

This statement, in and of itself, is a fair testament of how laborious the C4 interoperability process is and will continue to be into the foreseeable future (JCS/J6 2006). But, laborious as the process is, the JCS/J6 as the DoD Warfighter Chief Information Officer (CIO) goes on to spell out responsibilities for implementing actions to resolve these issues in the Joint Staff Joint Net Centric Operations Campaign Plan by identifying key tasks and offices of primary responsibility. This document supplements and supports the Chairman of the JCS's vision discussed earlier and can be viewed as the strategic vision of the Joint Staff in terms of C4 implementation across networks, radio systems, battlefield integration, satellite systems, and others. Within this document, Annex A, Goals, Objectives, and Actions identify specific activities and actions required to reach C4 interoperability in the joint environment. Following are extracts from the Joint Staff Joint Network Operations Campaign Plan:

Goal 1: Connect the Warfighter

Objective 1.4: Resolve **Interoperability** and Integration Issues Occurring Within the Operational Environment.

Joint Staff Division Lead: J6

Lessons learned from recent operations and DOD exercises provide critical feedback on system **interoperability**. OSD Operational Test and Evaluation Directorate (DOT&E) and Joint Staff/J6 Joint Tactical Radio System (JTRS) will team to provide **interoperability assessments** during annual C/S/A sponsored exercises and identify shortfalls.

Goal 5: Synchronize Delivery of Network Capabilities

Objective 5.1: Advance Communication System Engineering and Integration to Improve **Interoperability** and Supportability of IT and NSS

Joint Staff Division Lead: J6I

Objective 5.8: Collaborate With Allied and Coalition Partners to Develop and Implement Policies, Procedures and IT Standards That Promote Combined **Interoperability** *Joint Staff Lead: J6B.* (Chairman, Joint Chiefs of Staff 2006, 29-39)

The Joint Staff role in implementing C4I interoperability across the services and amongst our coalition partners is clearly defined in their campaign plan discussed above, but it doesn't stop there. The next higher level in the DoD chain of command is responsible to "ensure the interoperability of IT, including NSS, throughout the Department of Defense" (DoDD 5144.1 2005, 3). This office belongs to the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO), more commonly referred to as the DoD CIO in the communications and information community and for the purpose of this paper.

The DoD CIO is also responsible to "provide policies, oversight, guidance, architecture, and strategic approaches for all communications and information network programs and initiatives on an enterprise-wide basis across the Department, ensuring compliance with the information assurance (IA) requirements as well as interoperability with national and alliance/coalition systems. This includes network-centric and information-integration projects, programs, and demonstrations as they relate to GIG

implementation and employment" (DoDD 5144.1 2005, 5). This state, should in large measure, encapsulate all the DoD partners who have, or will have, interoperability issues which may now or in the future years require some level of C4 interoperability compliance and testing.

Since the DoD CIO is the "belly button" for C4 interoperability, which includes coalition partners, it is necessary to understand how a system becomes certified from inception through design and onto fielding as it parallels the acquisition process all major programs follow in the Program Objective Memorandum (POM) cycle.

Combined C4 interoperability is a difficult area to measure as it cuts across systems of systems, service departments, countries, classification levels of information, technical standards, networks, radio systems, satellites, and ultimately dimensions. In order to determine if a system is C4I interoperable, a measurement must take place in one of two ways, either through a test performed by JITC following their rigorous testing phases or an operational exercise between two previously known incompatible systems.

One of the largest C4ISR experiments in the DoD is known as the Joint Expeditionary Force Experiment (JEFX), which identifies warfighter technological gaps, tests solutions, and quickly fields (eighteen months) new hardware and software to the field to fill the gap. This Chief of Staff of the Air Force sponsored experiment is based within a test Combined Air Operations Center (CAOC) located at Nellis Air Force Base, Nevada, and has been conducted for seven, eighteen-month spiral development cycles since its inception (JEFX 2007, 1). JEFX participants include units that are geographically separated from the Nellis CAOC and many times include Air Force fighters, bombers, and reconnaissance aircraft to fully test newest capabilities brought

forward by DoD sponsored corporations. Underlying all of this effort is the fact that newly tested systems must be interoperable with existing systems and future systems otherwise the effort is a waste of time for everyone involved in JEFX. Although JEFX is Air Force sponsored, many of the newest systems answer the needs of Soldiers, Sailors, Airmen, and Marines following the extensive tests scheduled during the three-to-four-week-long experiment (JEFX 2007, 1).

Other methods of rapid technology insertion exist outside of normal acquisition channels and meet the JITC certification process requirements as well as the technical interoperability checks. Some of these include: Advanced Concept Technology Demonstrations (ACTDs), Coalition Warfare Program (CW), Defense Acquisition Challenge Program (DACP), Technology Transition Initiative (TTI), Quick Reaction Special Projects (QRSP), Foreign Comparative Testing Program (FCT), Rapid Action Initiative-Net Centricity (RAI-NC), Coalition Warrior Interoperability Demonstration (CWID), Air Force Combat Capability Documents (CCDs), Army Operational Needs Statements (ONSs), Marine Corps Urgent Universal Need Statements (U-UNSs), and Navy Rapid Deployment Capability (RDC) (CJCSI 6212.01D 2006, C-7). Like JEFX, these avenues allow the services to quickly field technology directly to the warfighter and still fill the need for C4 interoperability with existing systems already in use in the field.

Although these avenues work well for just-in-time technology insertion, the process for gaining JITC interoperability certification exists and is required for all other systems, which will touch the network. This can be a simple router or switch on an Army network stateside or overseas or as complex as the Army's Future Combat System (FCS), which incorporates a multitude of manned and unmanned vehicles using wireless

networking. Nevertheless JITC, working with the Defense Information Systems Agency (DISA), uses a very meticulous process of milestones and checkpoints to ensure each and every system goes through a corollary series of technical checks prior to being issued final certification. The JITC certification process is depicted in figure 1.

During the interoperability test process "JITC will evaluate the four Net-Ready Key Performance Parameters (NR-KPP) elements: compliance with the Net-Centric Operations and Warfare (NCOW) Reference Model (RM), supporting integrated architecture products required to assess information exchange and operationally effective use for a given capability, compliance with applicable Global Information Grid (GIG) Key Interface Profiles (KIPs), and verification of compliance with DoD information assurance requirements. In addition, service and agency operational test agencies may provide assessments of the operational effectiveness of information exchanges based on operational test events or exercises" (CJCSI 6212.01D 2006, E-4). Each system must complete both the Joint Interoperability Test Certification and the Joint Staff J6 System Validation before being fielded. Certification is valid for three years and must be renewed thereafter for life of the system (CJCSI 6212.01D 2006, 3).

The Program Manager (PM), likely a DoD employee, must follow this process to ensure his or her program meets the interoperability requirements for the JITC certification and also the JCS/J6 system validation. This sounds like a lot, but taken apart piece by piece it may make more sense and indicate the necessity of each step in the process. One of the easiest ways to get a system JITC certified is by association with another C4I system that has already completed the certification process and meets the data architecture requirements in DoD Architecture Framework, Volume 2, Product

Descriptions. Failing this, all C4I systems must go through the certification process as depicted in figure 1.

"The JITC Interoperability Test Certification process comprises four basic steps. Joint interoperability testing and evaluation is an iterative process--some or all of the steps may need to be repeated as conditions change. The four basic steps are:

1. Identify (Interoperability) Requirements
2. Develop Certification Approach (Planning)
3. Perform Evaluation
4. Report Certifications and Statuses (CJCSI 6212.01D 2006, E-4).

The first step of the JITC Interoperability Test Certification process requires the PM to submit initial requirements and capabilities of a C4I system within a document called the Initial Capabilities Document (ICD). The ICD is the source document which is staffed through the J6 and indicates whether proper certification and testing has been completed and if the system is non-fatal to the GIG as spelled out in the voluminous DoD instructions and J6 validation and certification requirements. If the system fails to meet these requirements, the ICD is held up from funding by the J6 until the issues are resolved. Many times, systems are incrementally improved in a spiral and may not meet the stringent interoperability test steps as required, which ultimately stalls certification progression. This first step of the process is pivotal to the PM in order to get program acquisition underway. The acquisition process is separate and distinct from the JITC Interoperability Test and Certification process and is not discussed within the confines of this study due to the complexity of the acquisition process. For the purpose of this paper, it is important to note, only that failure within this step halts funding by J6.

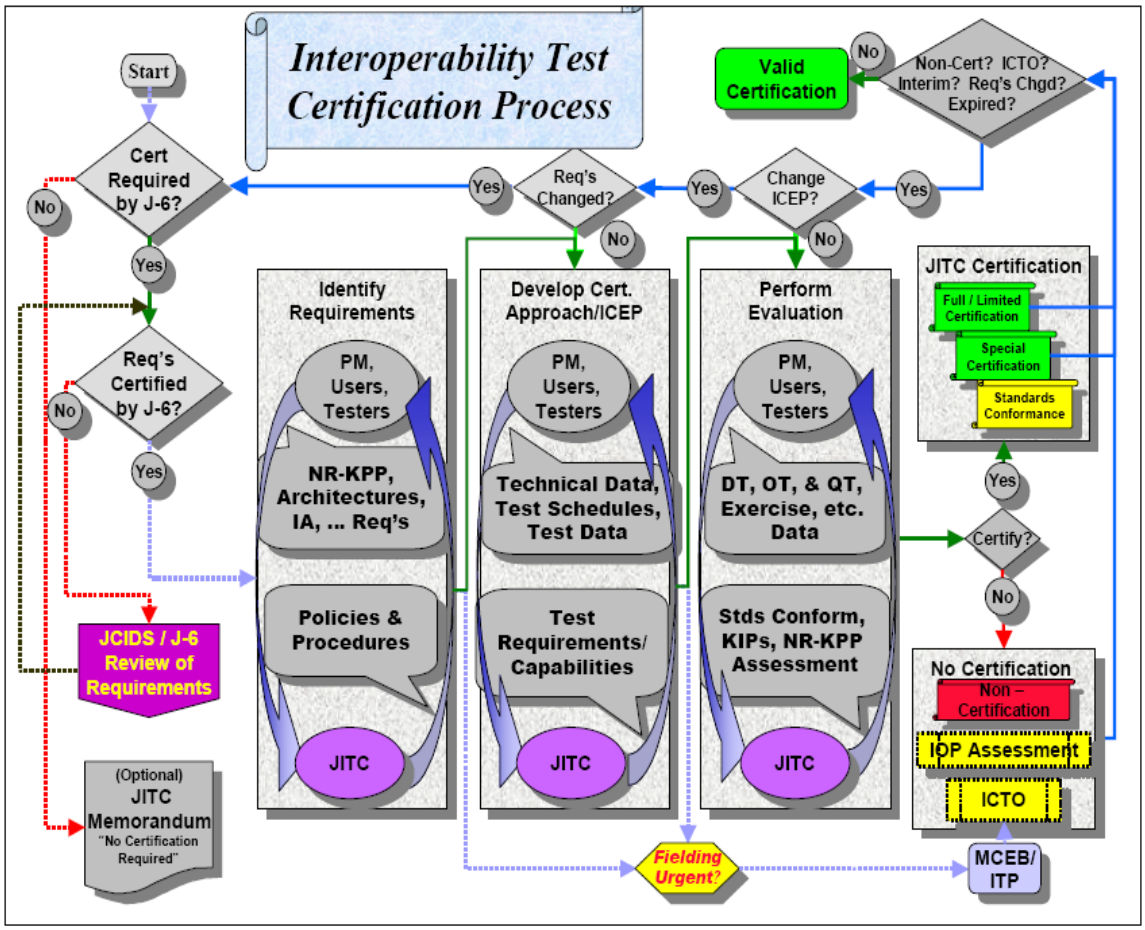

Figure E-1. Interoperability Test Certification Process

Legend:			
Cert	Certification	KIP	Key Interface Profile
DT	Developmental Test	MCEB/ITP	Military Communications-Electronics Board/Interoperability and Policy Test Panel
IA	Information Assurance	NR	Net-Ready
ICEP	IOP Certification Evaluation Plan	NR-KPP	Net-Ready Key Performance Parameter
IOP	Interoperability	OT	Operational Test
ICTO	Interim Certificate to Operate	PM	Program Manager (Sponsor)
JCIDS	Joint Capabilities Integration and Development System	QT	Qualification Test
JITC	Joint Interoperability Test Command	Req's	Requirements
J-6	Joint Staff J-6	Std's	Standards Conformance

Figure 1. Interoperability Test Certification Process

Source: Joint Chiefs of Staff, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01D, *Interoperability and Supportability of Information Technology and National Security Systems* (Washington, DC: Government Printing Office, 2006), E-6.

Another key part of the first step of the interoperability process is for the PM to ensure the C4I system meets the requirements of the Net-Ready Key Performance Parameters (NR-KPP). "The system must support Net-Centric military operations. The system must be able to enter and be managed in the network, and exchange data in a secure manner to enhance mission effectiveness. The system must continuously provide survivable, interoperable, secure, and operationally effective information exchanges to enable a Net-Centric military capability" (CJCSI 6212.01 2006, D4). This step is important as it lays the groundwork for system interoperability within the confines of the GIG so as to ensure network interoperability whether the system is used on land, sea, air, space, or cyberspace as well as across the many different platforms of C4I communications. These broad parameters also tie into the network architecture of the GIG to ensure survivability of military communications as specified and tasked by the J6 and DISA through the JITC. If these NR-KPPs are not met during the first step of the interoperability process, then the ICD is returned to the PM for further refinement with the sponsors of the system, who are likely representatives from industry and military contracted communications companies.

The second step of the JITC Interoperability and Test Certification process is to develop the certification approach or planning whereby the sponsor and user community jointly plan for controlled testing of the C4I system. "The sponsor and JITC will work closely to establish a strategy for evaluating interoperability requirements in the most efficient and effective manner, in an operationally realistic environment (the environment must be as operationally realistic as practicable--this includes employing production representative systems, members of the user community as operators, realistic messages

and network loads, configurations in compliance with IA requirements, etc.)" (CJCSI 6212.01D 2006, E-5). The results of these tests indicate whether the system meets the architecture, data, and system interoperability requirements spelled out in CJCSI 6212.01D and other DoD directives.

Complex C4I systems, like the air, missile, and space systems used by the North American Aerospace Defense Command within Cheyenne Mountain Air Station, Colorado, rely on this critical step of the JITC Interoperability and Test Certification process. Hundreds of test, operations, and communications and information personnel perform deliberate tests to safeguard the sovereignty of North America. The interoperability of these systems depend upon successive and well-documented system tests to ensure new software is interoperable, reliable, and meets the requirements of this critical step in the JITC process.

The third step of the JITC Interoperability and Test Certification process is the execution of the test plans developed during step two of this involved process. Typically the execution of a test is characterized by the relationship of the system to "go live." Developmental, Operational, and Qualification Tests take place in that order during step three. Test data is captured and operational integrity maintained in accordance with the test environment defined by the PM, operators, testers, and engineers. These efforts constitute a major milestone toward system interoperability compliance. Again, the NR-KPPs are evaluated in support of the protection of the GIG to ensure the military system in question is fully interoperable across the wide spread of communication domains. Once these hurdles are overcome, the C4I system is well on the way to becoming fully JITC certified during step four of the process.

The fourth step of the JITC Interoperability and Test Certification process is to report certifications and statuses. Not all systems tested meet the stringent interoperability requirements and do not become JITC certified, but all is not lost. The extensive and expensive tests completed during the process along with documentation serve as a ruler for the PM to go back and correct discrepancies through software and engineering changes or possibly reevaluate with the sponsors the true value of pursuing system improvements. The end result of this process assigns a certification label to the system as either certified or interim certification to operate (system not fully certified but will comply then be issued full certification). JITC then adds the system to their worldwide data base as a permanent record of the process results.

The JITC Interoperability and Test Certification process is essential to how the DoD, interagencies, and coalition members integrate the plethora of C4I systems in use today. Systems that fail this process are placed on the Interoperability Watch List in accordance with "DoD CIO, the Chairman of the Joint Chiefs of Staff, the Commander, U.S. Joint Forces Command direction to ensure that sufficient attention is given to achieving and maintaining interoperability objectives; and to provide DoD oversight for those IT activities for which interoperability is deemed critical to mission effectiveness, but interoperability issues are not being adequately addressed" (CJCSI 6212.01D 2006, GL-12).

Other C4I Interoperability Approaches

Although the JITC certification and JCS/J6 validation processes for interoperability are to say the least, comprehensive, critics favor a less cumbersome and more streamlined approach to meeting the same desired end state. Some of these critics

see the importance of tying all C4I systems together for the benefit of the field commanders and C2 agencies that support them by providing different approaches to attaining interoperability.

As cumbersome as the JITC and J6 processes seem, it may be beneficial to delve into current, alternate thoughts on C4I interoperability processes in industry, acquisition, and military channels to gain an appreciation for alternate solutions to attaining the same goal in support of the warfighters. Two alternative approaches to interoperability concentrate on "score cards" to prove whether systems are truly interoperable.

One of these alternative approaches was developed by three military officers (Lieutenant Colonel John A. Hamilton, Jr., USA, Captain Jerome D. Rosen, USAF, and Major Paul A. Summers, USAF) who worked for JITC and published an article which appeared in *Joint Force Quarterly* in the Winter issue of 2002, titled, "An Interoperability Road Map for C4ISR Legacy Systems." Their approach asserts that a necessary step in establishing interoperability across the multitudes of DoD C4I systems is to determine where each legacy system stands in relation to "full interoperability," then to apply a decision matrix to determine whether to continue or discontinue the program or system (Hamilton et al., 2002, 2).

The second approach, "Measuring Systems Interoperability: Challenges and Opportunities," was published by Mark Kasunic and William Anderson of the Software Engineering Institute, a federally funded research and development center sponsored by the DoD and affiliated with the Carnegie Mellon University. Kasunic and Anderson apply the Levels of Systems Interoperability model to interoperability and share detailed score cards, which indicate system compliance with a plethora of interoperability levels

and attributes (Kasunic and Anderson 2004, 4). Both score card systems represent a means of separating GIG compliant C4I systems based upon criteria established by a parent organization. The bottom line up front is that these are excellent methods of eliminating duplication in the C4ISR domain but these processes do not address C4I interoperability certification and accreditation as discussed earlier in the JCS/J6 validation and JITC interoperability certification processes.

To establish a common frame of reference in relation to C4I interoperability, a brief discussion of the Joint Technical Architecture (JTA), GIG, and standards is necessary. Following the publication of Black's thesis on C4I interoperability in 2000, CJCSI 6212 was rewritten in 2003 to include a reference from the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) in a memorandum on 14 November 1995. The memorandum tasked agencies of the services to "reach a consensus of a working set of standards" and "establish a single, unifying DoD technical architecture (TA) that will become binding on all future DoD C4I acquisitions" so that "new systems can be born joint and interoperable, and existing systems will have a baseline to move toward interoperability" (Department of Defense 2003, 27). The ensuing volumes of standards defined measures to achieve this interoperability and were subsequently absorbed into the DoD acquisition channels as directed to migrate existing systems and baseline new systems interoperability. Thus was born the JTA.

One of the main recommendations out of a variety of DoD sponsored C4I studies was the creation of a JTA. The JTA ties systems, sensors, networks, warfighters, and various airborne, seaborne, and land based platforms together using common standards and data fields (Department of Defense 2003, iv). Today, the JTA is defined within the

two-hundred and fifteen page DISA1, dated 3 October 2003, which established the methods, procedures, and architectural standards required to accomplish joint C4I interoperability.

DISA JTA Volume 1 defines architecture as the "structure of components, their relationships, and the principles and guidelines governing their design and evolution over time." In order to break the architecture into manageable components, the DoD established "interrelated set of views: operational, system, and technical" (Department of Defense 2003, 27). Each of these views is associated with a unique architecture as it applies to one of five domains (C4ISR, Combat Support, Modeling and Simulation, and Weapon Systems). This study focuses on the C4ISR domain only and has confirmed that all five domains are adequately addressed in the DISA JTA guidance. Focusing on the C4ISR domain and its associated technical view produces a JTA all its own and ensures full interoperability following the acquisition, development, and fielding of new C4I systems, as well as existing systems. Legacy systems are also able to meet the interoperability standards set forth in the JTA and therefore considered elemental to achieving information superiority for the warfighter.

The JTA addresses how to establish joint interoperability on new or improved C4I systems. "The DoD Joint Technical Architecture (JTA) provides the minimum set of essential standards that, when implemented, facilitates this flow of information in support of the warfighter. The JTA standards promote:

1. A distributed information processing environment in which applications are integrated.

2. Applications and data independent of hardware to achieve true integration.

3. Information transfer capabilities to ensure seamless communications within and across diverse media.

4. Information in a common format with a common meaning.

5. Common human-computer interfaces for users.

6. Effective means to protect the information.

The JTA defines the service areas, interfaces, and standards applicable to all DoD systems; its use is mandatory for the management, development, and acquisition of new or improved systems throughout the DoD" (Department of Defense 2003, 26). As in the case of the previously discussed JCS/J6 validation and JITC Interoperability Test and Certification processes, system interoperability is continuously reviewed and updated throughout the life cycle of the system. The JTA provides the necessary standards to ensure systems interoperate across the GIG as an interconnected system of systems. Although C4I interoperability is a very complex capability to establish, the JTA simplifies it by providing the bedrock through common interfaces and standards that work across the DoD, interagencies, allies, and coalition members who may require access or use of the wide variety of warfighter tools.

The JTA ensures that technical standards applied during the planning stages of system development are elemental and necessary to ensure full interoperability. Just as important are the test and development stages of the process wherein a legacy system reaches either full or interim interoperability. By understanding the process for interoperability certification and the standards used to validate it, the U.S. military services and coalition partners should be able to pool resources through the acquisition phases and reach some level of interoperability.

To validate this understanding, a review of joint C4I systems may aid in the discussion and highlight challenges currently facing PMs involved in the fielding, funding, testing, and development of joint programs. This study examined two ongoing joint programs, JTRS and DIMHRS, to see if the validation and certification processes are working as efficiently and effectively as possible. Chapter 3, "Patterns and Gaps in C4I Interoperability," discusses research approach and analysis methodology used in this study. Chapter 4, "Strategic C4I Interoperability Analysis," analyzes the JTRS and DIMHRS programs and determines the effectiveness of their associated research, development, funding, testing, and fielding processes since both of these programs have been in some form of development for over ten years.

CHAPTER 3
PATTERNS AND GAPS IN C4I INTEROPERABILITY

Introduction

This study uses a case study methodology to develop an understanding of progress made within the DoD in C4I interoperability. Case studies on two major joint programs, the JTRS and DIMHRS, provide a real-time glimpse into how the DoD has assimilated decades of criticism of their lack of deploying interoperable C4I systems.

Chapter 2, "Current State of C4I Interoperability," examines existing strategy and guidance from the national level down to each service in order to establish linkage between the strategic and operational levels of the DoD. This review includes a survey of law, strategy, objectives, and tasks to discover if gaps exist which may require revision due to changes in technology or doctrine associated with C4I interoperability. The JCS/J6 involvement with the JITC is mentioned as a key participant in JITC's four step system certification and accreditation process. The JTA is also summarized as the cornerstone of C4I interoperability and defined in terms of program management concerns.

Chapter 4, "Strategic C4I Interoperability Analysis," is the heart of this study and fully explores the JTRS and DIMHRS programs and then compares and contrasts each from an interoperability standpoint. Using the existing guidance, processes, and standards identified in chapter 2, it became possible to evaluate these two joint programs from inception through current day status in order to expose potential gaps. These gaps represent the answers to the primary research question. Each program, JTRS and DIMHRS, was broken down into like sections of background, integration, implications, interoperability assessment, and lingering lessons to set the stage for comparison and

contrast. In the interest of time and space, the comparison and contrast was incorporated within each program section to which it applied vice separately. Some sections on DIMHRS were combined to streamline the discussion as joint program management can be cumbersome to analyze and absorb. The similarities and differences discovered helped identify similar gaps in law, acquisition, strategy, and PM.

Chapter 5, "Conclusions and Recommendations," highlights and summarizes the most obvious and lingering gaps identified during the course of the study. Significant gaps in law, strategy, acquisition, and certification and accreditation processes were discovered in previous theses and studies and continue to linger to date. The impact of these gaps in C4I interoperability can be measured in time, cost, or performance from the PM standpoint. The single biggest failure is that even though the DoD has an appropriate amount of architecture, standards, commercial partnerships, DoD directives (DoDD), Joint Chiefs of Staff Instructions (CJCSI), and years of Government Accounting Office (GAO) reports from which to draw upon, it still has not achieved C4I interoperability across the services, with its allies, nor with coalition members.

CHAPTER 4
STRATEGIC C4I INTEROPERABILITY ANALYSIS

Introduction

The abundance of research conducted on C4I interoperability seems to dwell on determining if the U.S. and their allies should integrate methods, processes, and efforts to produce C2 systems that cut across service and country boundaries and provide relatively transparent "systems" for the execution of wartime missions. The resounding conclusion, as identified in Black's thesis, is yes. Therefore, this study focuses on the "how" rather than the "why" in today's very complex C4I environment. Although there are five domains within which each C2 system operates, it was necessary to focus on one domain (C4ISR) and "how" to best implement interoperability for the U.S. and its allies or coalition members.

Since the publication of Black's thesis in 2000, many improvements, both off-the shelf and DoD proprietary contracts took place that improved "how" the U.S. builds, funds, and deploys interoperable C4I systems. This distinction is necessary at this point in the study to explain the resultant methodology. This study will examine two existing joint systems (JTRS and DIMHRS) and look closely at "how" they met or did not meet the spirit and intent of the aforementioned certification and validation processes and standards from within the JTA. This study will begin with a macro view of interoperability, based in part on a U.S. Navy study on C2, as it drills down into the JTRS and DIMHRS programs.

The U.S. Navy commissioned a study, conducted by the Naval Sea Warfare Center in Crane, Indiana, which focused on military command and control (C2) systems, titled "Military Communications Strategic Insight," with an overall intent of providing a

roadmap toward future C2 interoperability. The study begins by defining C2 as "the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken" (NAVSEA 2005, 3). The report goes on to delineate the difference between C2 and other specialized functions like logistics, intelligence, electronic warfare, and administration by pointing out that all these functions in some manner or another touch and depend upon C2. In this light, "C2 encompasses all military functions and operations, giving them meaning and harmonizing them into a meaningful whole. It is essential to all military operations and activities. C2 helps commanders make the most of what they have-people, information, material, and, often most important of all, time" (NAVSEA 2005, 4). This distinction is important when constructing a "system of systems" to achieve interoperability. C2 encompasses almost every information system in the DoD inventory, but the Navy report focuses on a picture in time to evaluate JTRS progress.

The Crane team, authors of this report, found that the "estimated C2 market value over the next decade is $200 billion dollars" (NAVSEA 2005, 3). They further discovered that there were three common factors that drive the market: "the IT revolution, the need for a seamless and interoperable - more affordable - C2 capability, and our country at war" (NAVSEA 2005, 3). Understanding the changing dimensions of the IT revolution and its impact on C2 development within DoD systems dramatically improves the possibility of eliminating interoperability woes. Likewise, focusing on the interoperability issues associated within the DoD, C2 systems would not only improve system interoperability among the services, but also for the U.S. allies and coalition members. Fielding C2 systems during a major war can in many ways improve

interoperability since the systems are fielded to troops in battle. Most Americans would probably prefer the U.S. fields "tested" capabilities when those systems directly involve the safety of Soldiers, Sailors, Airmen, and Marines.

The Crane report identifies these factors to illuminate the fact that they will continue to "change and shape the acquisition strategies for C2 equipment, systems, and networks. This is most illustrated in JTRS, which will render most current equipment obsolete. Systems and networks complete this capability and present an even more complex challenge of bringing diverse communities and needs together" (NAVSEA 2005, 3).

The findings of the report provided detailed insight into how commercial companies contributed to military C2 production and offered some interesting conclusions about C2 investments within the DoD in 2005. "Two hundred forty-five unclassified military communications programs (U.S.) in various stages of development were identified. All DoD Services are involved and fifty-two of the programs were multi/joint service participation. Twenty-three programs involved international forces. Five Advanced Concept Technology Demonstrations (ACTD) programs are included. As for market share, approximately 22 percent of contracts are widely dispersed among small business participants or within less notable divisions of major industry contractors. Garnering the top three shares were (percentages approximate):

Raytheon .....…16.8%

Rockwell-Collins .....…11.5%

Harris 6.5%

Though not holding a very significant market share by volume, Lockheed Martin and Boeing seem to have locked in the more monetarily significant contracts, specifically the JTRS program. In the next decade, it is likely that the communication industry will become more consolidated and specialized. Many disparate and service centric equipment and systems will be replaced by JTRS and an ad-hoc networking capability" (NAVSEA 2005, 4). Figure 2 provides a pictorial view of how JTRS springboards common joint communications platforms in the air, on the seas, and on land into one GIG network and shows how it must be interoperable to function properly. Herein lies the essence of interoperability for communications systems involving any facet of C4I. A complete study of the JTRS program from inception, through acquisition, and onto fielding may indicate how successful the DoD is considered in implementing true interoperability standards, architecture, and equipment across the services and amongst U.S. allies and coalition partners.

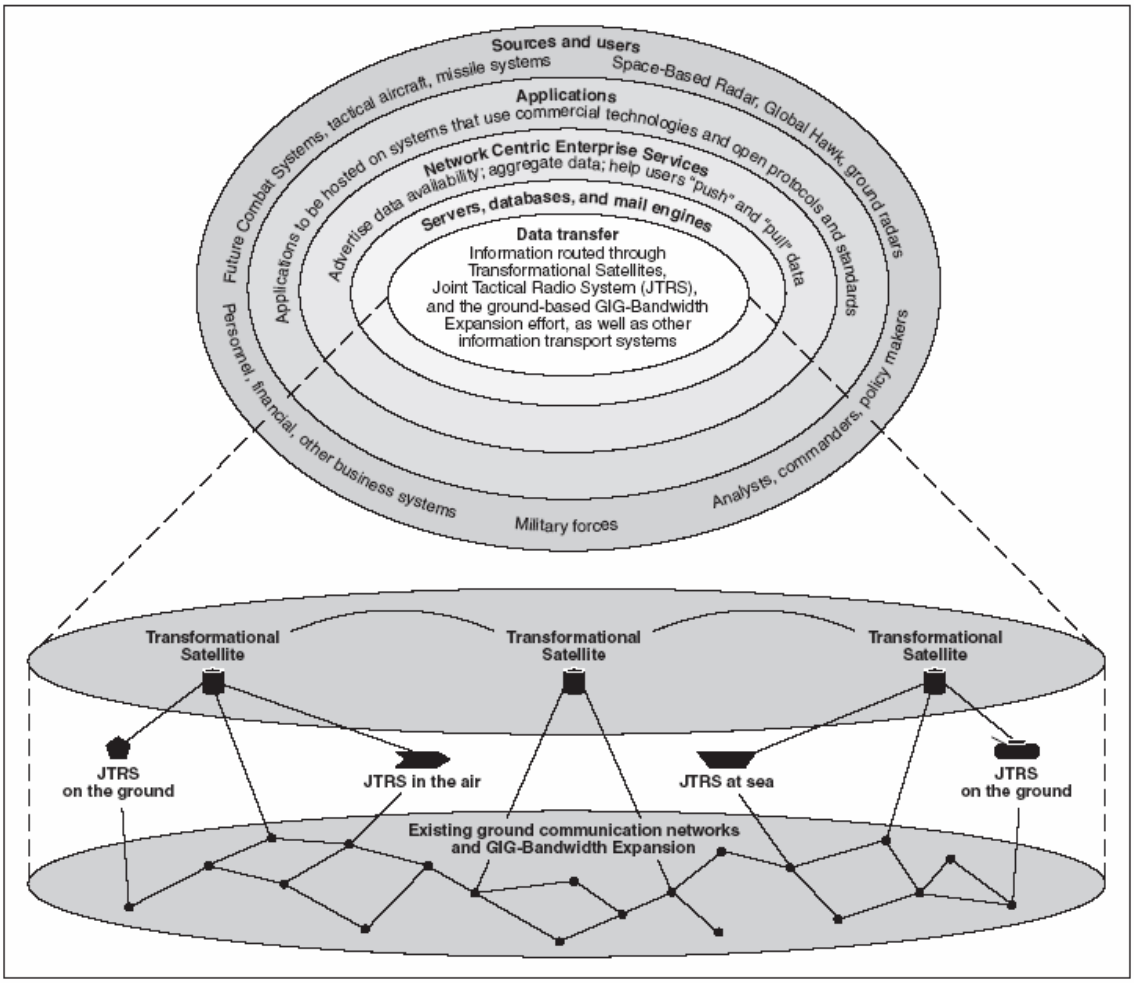

Figure 2. JTRS Network

Source: Naval Sea (NAVSEA) Warfare Center, *Military Communications Strategic Insight* (Crane, IN: Government Printing Office, 2005), 6.

JTRS Background

If JTRS was a replacement radio system, how did it become a GIG network foundation replacement for DoD? The JTRS program was initiated in 1997 as a radio replacement to the numerous radios each service used throughout their land, air, and sea operations. This family of radios was to be fielded in clusters, managed by separate services, of technology over several years in order to field radios in a quicker manner. As

the JTRS office worked laboriously on the abundant technological challenges of replacing hundreds of different radio waveforms and specifics from an equal number of contracted companies, doctrine was undergoing changes as well. The call for transformation across the DoD resounded throughout the services and the JTRS program management office also heard it and was very quickly tasked to adjust its focus from that of radios to the entire GIG.

The JTRS office was notified of this change to become the "last tactical mile" in the GIG and to lay the foundation for "net centricity." The question becomes what has happened or not since that time? Why the lengthy delay? Did the JTRS office actually field any radios or network devices compliant with this strategic investment and acquisition plan? Which service is actually leading the charge on the various network platforms depicted in figure 2? Where does a customer go to find out the status of its new radio system and when it may be fielded? These are not unusual questions to ask a PM who has managed a program for a number of years. By answering these questions a clearer picture should evolve of how these interoperability processes become interdependent and sometimes intertwine to thwart progress.

GAO report number GAO-03-879R, *Challenges and Risks Associated with the Joint Tactical Radio System Program*, briefed, as requested, the Deputy Assistant Secretary of Defense (C3, Space, and IT Programs) on 5 May 2003 (GAO-03-879R 2003, 2). This was the first official written report summarizing the JTRS program efforts to field the various clusters of radios across service lines and incorporated the new direction for a newly formed joint program office. The GAO report found "the JTRS program is considered a major transformational effort for the military and is expected to enable

information superiority, network-centric warfare as well as modernization efforts, such as the Army's Future Combat System. Although total program costs have yet to be determined, the Army's effort to acquire and field close to half of the estimated 250,000 JTRS radios that are needed is expected to cost $14.4 billion" (GAO-03-879R 2003, 3). The JTRS program not only picked up the additional responsibility of solving "net-centricity" or migrating all devices onto the GIG, but it also became an integral part of the Army's FCS composed of unmanned aerial and ground vehicles. This insight, in 2003, levied more importance onto the JTRS program for solving what many would call an interoperability issue but at the same time expanded its breadth and depth of responsibility.

The GOA report went on to identify some of the strengths and weakness of the JTRS program in 2003. The strengths were:

> Joint Program Office has been established to bring together the services' individual efforts to develop software-defined radios.
>
> PM developed a standard software communications architecture that provides a foundation for building JTRS radios and evolving an open systems approach to facilitate technology insertion.
>
> PM reduced risk by employing an evolutionary acquisition strategy, whereby improved communications capabilities will be delivered in increments. (GAO 03-879R 2003, 3)

These strengths were well known by the community of interest at the time, and publishing them simply became a matter of fact. They did serve as a beginning to what still exists as a long and difficult task. The weaknesses, on the other hand, provided new insight into what may improve future progress and put authority where it was needed most in the JTRS program, at the PM level. The GAO report made the following recommendations to strengthen the JTRS program:

1. Establish centralized program funding.

2. Realign the Joint Program Office under a different organizational arrangement.

3. Placing the cluster development programs under the Joint Program Office control (GAO-03-829 2003, 3).

Additionally the GAO also made the following recommendations to the Secretary of Defense:

1. Direct the completion of key program documents detailing the program's [JTRS] vision.

2. Make sure key enabling technologies, such as networking capabilities, are adequately addressed.

3. Assess the impact that the continued purchase of existing radios may have on JTRS. (GAO 829 2003, 4)

Whereas previously the JTRS program was spread widely over all four services and throughout a vast array of contracted suppliers across the country with little to no centralized management, the GAO concluded this detracted from good stewardship of public accountability. Seemingly important as the technological challenges were the fiscal challenges, which were stovepiped by service dependent upon the cluster of technology each managed for their own future capability. The Secretary of Defense disagreed with this GAO finding and maintained it would be best to let the services independently fund their cluster development rather than pool funding under one joint program management office.

The GAO directed the Secretary of Defense to get control of the myriad of processes within the JTRS program, focus them on what would become later known as

"netcentricity," and consider the alternative of JTRS radios now that the overall emphasis of the JTRS program was recast from its original charter. This dramatic evaluation in 2003 of the JTRS program began storms of transformation across the services and placed renewed interest on a program, which was originally chartered as a joint radio replacement plan.

The federal government understood the importance of JTRS to C4I interoperability and the GIG, and that insight was reflected in the GAO report. This document began a revolution of sorts within the services to reevaluate their role in JTRS "cluster management" and what, indeed, the technology they thought they were paying for and developing could possibly be recast into as related to this new JTRS charter. Knowing this piece of JTRS history begins the discussion of where the program is today and how it got there.

JTRS, formed in 1997, was originally designed to "improve and consolidate the Services' pursuit of separate solutions to replace existing legacy radios in the DoD inventory. JTRS evolved from a loosely-associated group of radio replacement programs to an integrated effort to network multiple weapon system platforms and forward combat units where it matters most - the last tactical mile" (JPEO 2006, 1). The GAO findings in 2003, which recommended the Secretary of Defense establish a joint program management office to oversee JTRS development; it was not until 2005 that "JTRS was restructured under the leadership of a Joint Program Executive Officer (JPEO) headquartered in San Diego, California" (JPEO 2006, 2).

The JPEO set the new vision, as directed by the GAO 2003 report, to reflect the JTRS "new" direction in that it would "link the power of the Global Information Grid

(GIG) to the warfighter in applying fire effects and achieving overall battlefield superiority" by producing a family of "interoperable, modular, software-defined radios that operate as nodes in a network [GIG] to ensure secure wireless communication and networking services for mobile and fixed forces. These goals extend to U.S. allies, joint and coalition partners, and, in time, disaster response personnel" (JPEO 2008, 3). The JTRS JPEO staff was established, provided its new vision, and laid the bedrock for an interoperable network across service lines and international borders for the first time in history. Much work remains to be done to reach this goal but defining the mechanisms, processes, money, testing, fielding, and relative levels of effort to get there were now under a single umbrella within DoD. Figure 3 provides currently developed JTRS equipment, which will support forces in the air, on land, or on the sea.

Airborne, Maritime, and Fixed Site (AMF)

AMF units are 4-channel, full duplex, software-defined radios that will be integrated into multiple classes of airborne, shipboard, and fixed-station platforms, enabling maritime and airborne forces to communicate seamlessly and with greater efficiency through implementation of five initial waveforms (i.e., UHF SATCOM, MUOS, WNW, SRW, and Link-16). AMF will provide data, voice, and networking capabilities to aircraft such as the Air Force C-130, Army Rotary Wing, and Navy E-2, along with maritime and shore sites.

Multifunctional Information Distribution System (MIDS)-JTRS

MIDS-JTRS is a wireless, jam-resistant, and secure information system component that provides real time information and situational awareness to the warfighter in fast mover platforms (e.g., Navy F/A/18, Air Force F-22) via digital and voice communications. An evolutionary development of the initial MIDS Low Volume Terminal to be JTRS compliant in the same form factor, MIDS-JTRS is a modular 4-channel radio providing Link-16, JAN-TE, voice, and next generation data and communication terminals for joint and coalition tactical platforms.

Ground Mobile Radios (GMR)

GMR is a 4-channel, software-definable, multimode communications system designed to support warfighters in ground vehicles such as the Bradley, M-1 Abrams, and MRAP. Providing the communication backbone of the Army's FCS, GMR, via software generated waveforms, provides a means to communicate with other JTRS radios and legacy systems, by bridging or cross-banding, thereby improving communications and information sharing among warfighters. GMR technology includes the new Wideband Networking Waveform (WNW) that has the capability to transfer internet protocol packets to other systems as well as ad hoc networking.

Handheld, Manpack, and Small Form Fit (HMS)

The future of tactical radio communications is being defined by the need for smaller, lightweight, and more powerful devices that are interoperable using a common software language. HMS is developing small form fit factors that provide tactical networking for solider carried 2-channel handhelds and manpacks, unmanned ground vehicles, munitions and sensors, and UAVs. These radios will enable cost-effective net-centric warfare to move beyond the command center to battlefield locations previously unreachable by legacy technologies.

Consolidated Single-Channel Handheld Radios

Currently available are two handheld, single-channel, software-defined radios developed for use by U.S. Special Operations Command, U.S. military services, and NATO Special Forces. These radios - the AN/PRC-148 and the AN/PRC-152 - enjoy interoperability with other military radios and commercial systems through their instantiation of legacy waveforms (e.g., SINCGARS, HaveQuick II). NSA Certified and considered "JTRS approved," they are presently deployed in combat, aiding U.S. warfighters in Iraq and Afghanistan.

Network Enterprise Domain (NED)

The goal for the NED Program Office is to develop and deliver portable, interoperable, transformational networking waveforms (e.g., WNW, SRW, JAN-TE), as well as the software to manage the network services needed to fully enable JTRS' mobile, ad hoc networking capability. NED products will produce the networking capability that allows U.S. warfighters from all military service branches to access and share relevant and timely information. This program is the heart of the interoperable networking capability of JTRS.

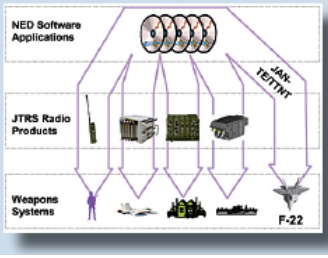

Figure 3. JTRS Equipment

Source: Joint Program Executive Office (JPEO) for Joint Tactical Radio System (JTRS), "Connecting the tactical edge," http://jpeojtrs.mil/files/org_info/ JTRS_Fact_Sheet.pdf (accessed 8 April 2008).

JTRS Integration

The JTRS technology, although slowly implemented, began picking up developmental speed and congressional interest since the beginning of the Global War On Terrorism. Congress, at the behest of its constituents, continues to demand the best for troops on the ground in Iraq. Since the JTRS program is a central part of the GIG migration strategy, it gets renewed interest and attention. The Army's FCS, composed of manned and unmanned vehicles and a host of wireless networking capabilities, works closely with the JTRS office as a "cluster" manager by fielding "Spin Outs" quicker to Soldiers in Iraq (Department of the Army 2008, 1). These Spin Outs are a method of rapidly fielding new technology onto the battlefield.

The Spin Outs put new technology where it is intended as soon as it is tested and deemed safe to operate. This new approach to acquisition and development has paved the way for radical technological changes in capability in much shorter time frames and speeds overall program development efforts. FCS provides soldiers in Iraq with the latest weapons and the Spin Out acquisition process is the Army's tool for quickly delivering new developments. "The FCS equipment and technology gives them unmatched situational awareness and survivability during conventional and asymmetric warfighting." Within Spin Out 1, the Army's Evaluation Task Force will evaluate a cluster of JTRS radios to ensure they integrate properly with the soldier on the ground and the various unmanned aerial vehicles (Department of the Army 2008, 1). Although the FCS fielding for the "first FCS Brigade is slated for fiscal year 2015, FCS technology is being accelerated to the Army's modular brigades through Spin Outs."

FCS, on a par with JTRS, is a large program headed by a two-star general program manager and a one-star deputy with over one third of the Army's annual research and development budget making it the largest program in DoD. The Army defends the FCS price tag of $260B as justifiably affordable since it only uses one third of the annual budget. FCS requirements are routinely changed to reflect new wartime needs identified during the Global War on Terrorism. FCS follows the rules for JTA interoperability from design to current day test and evaluation of over 75 FCS systems and capabilities. "The FCS Small Unmanned Ground Vehicle and the Class 1 Unmanned Aerial Vehicle Block 0 have entered accelerated testing by Soldiers at the Army Evaluation Task Force. Testing is set to conclude in the fall 2008, when FCS and Army capabilities managers will provide recommendation on whether to field the platforms or continue system development under the core FCS program. The first FCS Manned Ground Vehicle prototype, the Non Line of Sight-Cannon will debut in June 2008" (Department of the Army 2008, 2).

The FCS impact on JTRS fielding and vice versa is likely to occur in the near future should the technologies collide, however, given the aggressive testing and fielding processes the resultant effect may be minor. Knowing that within the DoD in 2008 there are two large, interdependent, interoperable, multiservice, and joint programs well underway signifies a new horizon for C4I interoperability across all domains. FCS just happens to be the Army's solution while JTRS is a joint DoD solution.

JTRS Implications

JTRS JPEO brought all program management, acquisition, and development under centralized control with decentralized execution due to the size and complexity of

the software requirements for each community of interest. Since inception of the JTRS, JPEO a revised acquisition strategy took hold to control cost overruns and function deconfliction among the three platforms JTRS will ultimately support (air, land, and sea). An incremental acquisition deployment strategy is culturally sound to the DoD yet less risky, which provides agencies like the GAO with some semblance of confidence. This, however, is an acquisition strategy, which neither encourages interoperability across the services nor puts the technology where it needs to be in the shortest amount of time. In a decade where the DoD "plans to invest $1.4 trillion in major weapons programs" and "the GAO has found that the department has failed to deliver weapon systems on time, within budget, and with desired capabilities," it becomes clear that C4I interoperability is only a slice of weapons system program management challenges facing the DoD (GAO-07-388 2007, 1).

JTRS interoperability progress is inherently related to the DoD acquisition and development process in the big picture. In order to understand why complex weapons system development and fielding takes so long, as it has with JTRS, it is necessary to understand the acquisition processes involved in deploying military capabilities. The President, his staff, and the Joint Chiefs of Staff direct the services to meet capability based requirements in the *NMS/NDS,* and that vision is echoed in the *QDRR* as a roadmap for the future. The Joint Capabilities and Integration System (JCIDS) is the JCS vehicle for directing capability development throughout the DoD and interagencies.

Once directed by JCIDS, the respective service lead for the capability then absorbs the requirement into its own unique service strategy and the acquisition begins. The GAO report titled, *Integrated Portfolio Management Approach to Weapon System*

Investments Could Improve DoD's Acquisition Outcomes, March 2007, found that corporate industry does a much better job of acquisition and development than the DoD. The commercial industry manages product development through critical risk, financial, and management evaluations across the entire corporation, whereas the DoD stovepipes acquisition and development by respective service which creates duplication of effort and expense (GAO-07-388, 2007, 2).

The Senate Armed Services Committee, in a letter contained within the GAO report, commented on the acquisition dilemma and asked the GAO to investigate how the DoD might incorporate "best practices" from the civilian industry to overcome DoD shortfalls in the future. "In fiscal year 2006, the Senate Armed Services Committee raised concerns that DoD's poor track record with acquisition programs was linked not only to the department's Defense Acquisition System (DAS) for managing product development, but also to the department's Joint Capabilities Integration and Development System (JCIDS) for identifying the warfighters' needs and the Planning, Programming, Budgeting and Execution process for allocating resources" (GAO-07-388 2007, 2). The GAO report concluded that in order for the DoD to have enterprise level oversight of the multitude of platforms it manages in the joint and service communities, it must adopt a new acquisition and development scheme, similar to the industry approach of portfolio management. This report baselines a core problem across the DoD and emphasizes why true interoperability within the DoD, its services, coalition members, and allies remains an elusive goal.

Fiscal levity is the essence of any survivable weapons system within DoD, and therefore becomes the primary discussion item when considering changes to existing

acquisition and development processes. The GAO noted that although the DoD indicated it "would experiment" with portfolio management, their "initiatives are likely to face the same fate because they do not fundamentally change DOD's service-centric framework or sufficiently integrate its decision-making processes for making weapon system investments" (GAO-07-388 2007, 34). Since the JCIDS process determines what capabilities need to be developed yet counts on the respective lead service to pay for it out of its own budget, it is not surprising that the end result is a service unique capability with little emphasis on interoperability, C4I or otherwise.

JTRS implications are notwithstanding technological coordination as discussed previously in the J6 and JTIC certification and accreditation processes. The technical application of standards identified within the JTA are in place and functioning properly; however, the fiscal management of either joint (JTRS) or service unique capabilities (FCS) still resides within the lead service. So long as there are no compelling hands-on management organizations at the JCS level to produce fiscal and legal responsibilities, interoperability disconnects will continue to plague the DoD, coalition members, and allies. JTRS limited progress is proof of continual program slips, technological course changes, and fiscal cuts. Before JTRS can become a bedrock program of the GIG, it will require centralized control and decentralized execution within the acquisition and development communities. Short of this, JTRS can only make incremental progress as longer delays equate to increased technological changes, which add to production costs.

JTRS Interoperability Assessment

The JTRS program reorganization, under a JPEO, impacted program management and more importantly affected the C4I interoperability equation amongst the services,

coalition partners, and allies. In 2006, the GAO was summoned to evaluate if the recent JTRS reorganization met its goal of creating centralized control and to identify any risks to its successful fielding. "The JTRS program has encountered a number of problems, resulting in significant delays and cost increases. The program is currently estimated to total about $37 billion" (GAO-06-955 2006, 1)

The GAO determined that the JTRS program, under joint management, is making progress from a management perspective, however, shortfalls in technology development, budgeting, and interoperability still thwart future progress. "Operating in a networked environment--open to a large number of potential users--has also resulted in a lengthy, technically challenging, and still evolving information assurance certification process from the National Security Agency. [*Furthermore, the proposed interim technical solutions for enabling network interoperability among different JTRS variants have yet to be designed and developed.*]" (GAO-06-955 2006, 3).

Overcoming the extraordinary feat of combining management functions from across the services and commercial industry under one joint umbrella turned out to be a difficult task, but necessary. With centralized control of the JTRS program, its JPEO now has oversight and management of all the moving pieces and parts that support JTRS development of air, land, and sea based technologies. The GAO echoed this fact in their report and linked it to a reduced set of risks to the JTRS program along with a description of the new incremental development strategy. Similar to the FCS Spin Out process, JTRS incremental development produces products as technology allows vice striving for an unknown, unattainable end state, which was the case pre-JPEO as depicted in table 1, extracted from the GAO report.

Table 1. JTRS Program Changes

Table 6: Summary of JPEO-Initiated Changes to JTRS Program

Parameter	Pre-JPEO	JPEO
Management Structure	Decentralized	Centralized/Enterprise
Requirements Approach	Unconstrained (Big Bang)	Constrained (Incremental)
Program Milestones	Compressed	Expanded
Waveform Deliveries	Expansive	Reduced
JPEO Assessment of Program Risk	High	Moderate

Source: GAO analysis.

Source: Government Accountability Office, GAO-06-955, *Defense Acquisitions: Restructured JTRS Program Reduces Risk, but Significant Challenges Remain* (Washington, DC: Government Printing Office, 2006), 15. http://www.gao.gov/new.items/d06955.pdf (accessed 28 October 2007).

A central JTRS interoperability issue today is the waveform developments required to support operations in air, on land, and sea. These software waveforms account for much of the JTRS $37 billion in research and development while the radios, which use this multi-platform software is relatively inexpensive in the grand scheme of the DoD budget. Again the question becomes one of progress in terms of getting to the desired end-state of fully interoperable radio platforms and basing netcentricity in the GIG? Rather than dwell on the status of the JTRS waveforms and any projected milestones, this study focuses on the overall management of JTRS, in the grand scheme of becoming interoperable across the DoD and amongst coalition members and allies.

As evident in table 1, the JTRS program milestones changed from a compressed to an expanded schedule, which meant lengthier delivery of the required capabilities. On the positive side, JTRS technological developments to date are fielded as soon as practical to the servicemen and women fighting the Global War on Terrorism in Iraq and

Afghanistan. The age-old question lingers as to when the DoD may attain full C4I interoperability. JTRS stands as a current day example of the challenges service unique and joint programs endure despite contractual requirements and political expectations of getting there sooner.

JTRS Lingering Lessons

JTRS is an example of a well intentioned joint program stalled amongst a plethora of DoD directives, guidelines, strategies, architectures, standards, policies, and exercises that otherwise could have expedited the delivery of its original capability objectives.

Lt Col Anthony W. Faughn, USAF, noted in his 2002 study with the Center for Information Policy and Research at Harvard University, titled *Interoperability: Is it Achievable?* that "complete interoperability will almost certainly never be achieved" in the DoD (Faughn 2002, 48). His study considered interoperability issues across the services and among coalition, multinational, and allied partners with a chapter devoted to "Factors Limiting Interoperability." In this chapter he identified the following roadblocks to interoperability: "acquisition culture, budgets, rapidly changing technology, changing nature of operations, priorities, and oversight" (Faughn 2002, 21).

The same lingering lessons that plagued the JTRS program during its inception in 1997 continue to thwart C4I interoperability progress today, as identified in Faughn's study. Namely budgets, rapidly changing technology, priorities, and oversight are almost identical in today's procurement cycles within the DoD. JTRS is a prime example (Faughn 2002, 21).

Black, as previously cited throughout this study, synopsized his characterization of the necessity of interoperability: "The areas of responsibility and interest are larger

due to increase communications connectivity. Improved technology in C4I systems now allows commanders to disseminate command and control decisions to intermediate levels of the battlefield much faster than previous conflicts or operations. Common equipment and common standards are the first step in making coalition interoperability the next logical step. [*C4I system interoperability is a necessity*.]" (Black 2000, 66) Although Black discovered many of the same roadblocks to C4I interoperability that Faughn did, he was optimistic that full interoperability is possible through programs like JTRS which move the DoD closer to realizing the GIG and full netcentricity.

Both authors are right when viewed from a JTRS standpoint. The best way to confirm either position is to evaluate another ongoing joint program which purports large interoperability requirements, consumed large amounts of the DoD budget, and taken many years to excite development, the DIMHRS.

DIMHRS Background and Integration

DIMHRS is a DoD personnel and pay system for the services and interagencies that highlights some C4I interoperability implications which surfaced during fielding. An in-depth look at DIMHRS background, integration, implications, and lingering lessons will uncover similar C4I interoperability issues discussed in the JTRS case study. As in the JTRS case, there is extensive reference to a variety of GAO reports completed since DIMHRS program inception in 2004 to provide an unbiased view of program progression. DIMHRS is not as complex as JTRS but ultimately depends upon those same qualities of success required to ensure compatibility among the services and in this case, the interagencies at some point in the future.

In 1995, a "Defense Science Board task force on Military Personnel Information Management was convened to advise the Secretary of Defense on the best strategy for supporting military personnel and pay functions. The Task Force's report concluded that the DoD multiple, service-unique military personnel and pay systems caused significant functional shortcomings (particularly in the joint arena) and excessive development and maintenance costs. To address these shortcomings, the Task Force recommended that the DoD transition to one, all-Service and all-Component, fully integrated personnel and pay system that uses the same core software with similar requirements. Once implemented, the DIMHRS will provide an end-to-end, integrated military personnel and pay system for all military Services including their Active, Reserve, and National Guard Components. DIMHRS is the vehicle for fielding and resourcing a fully integrated human resources system, while simultaneously supporting reengineered business processes, replacing failing systems, reducing data collection burdens, enhancing readiness, and connecting Soldiers, Sailors, Airmen and Marines directly to their personnel and pay system" (DIMHRS 2008, 1).

In a perfect world, DIMHRS will provide all personnel and pay services each service member depends on daily throughout the course of his or her career. Some of these capabilities are unique only to a given service yet must be dealt with under the DIMHRS umbrella. Therefore, there is a legacy aspect of DIMHRS which must be incorporated into the new program from each service in order to continue to maintain the levels of support Soldier, Sailors, Airmen, Marines, and Coastguardsmen have come to enjoy with their own personnel and pay systems. This is how DIMHRS began as a joint venture.

Known as an Enterprise Resource Planning System, "DIMHRS has less than 2% customization to the off-the-shelf PeopleSoft software" and is used by companies like Wal-Mart, FEDEX, and Toyota (DIMHRS 2008, 1). DIMHRS started during an era when the Secretary of Defense emphasized using existing commercial-off-the-shelf technology. Barring some cultural name changes, PeopleSoft software was selected to ramp up the DIMHRS program. Implementation was identified in three phases:

1. DIMHRS (Personnel/Pay)--military personnel hiring, promotion, retirement, and pay.

2. DIMHRS (Manpower)--workforce planning, analysis, and utilization.

3. DIMHRS (Training) (GAO189, 2005, 3).

Currently the Army's DIMHRS Program Office (ADPO) plans to implement a "properly tested and fully integrated personnel and pay system (DIMHRS) to all Army components with properly trained users in 2008" (DIMHRS 2008, 1). According to the DIHMRS website, the Air Force fielding decision ("go live" date) is scheduled for February 2009. Overall program management responsibility rests with the DIMHRS Enterprise Program Management Office, which is headed by a Senior Executive Service civilian employee. In addition to being managed by a General Officer equivalent, the DIMHRS program is also subordinate to the Defense Business Systems Acquisition Executive which is currently filled by a Major General, U.S. Army. This parallels the JTRS program management oversight which is also headed by a Major General and a Brigadier General as the deputy.

Northrop Grumman Information Technology is the developer and integrator who work closely with a team of over 200 people at the Space and Naval Warfare Systems

Command Systems Center in New Orleans, Louisiana, under the auspices of a multiyear, $281 million contract signed between the U.S. Navy and Northrop Grumman (DIMHRS 2008, 2). Given the fact that DIMHRS integrates processes, records, data, and customers from across the services and from over 80 legacy systems, a key decision for program managers centered on how systems would be "subsumed." In many instances, DIMHRS did not incorporate the older legacy systems to full capacity, so PMs decided that if "a system is 75% covered through DIMHRS . . . then the system will be subsumed. If we need the other 25%, we will either reengineer that functionality or figure out a way to include it in DIMHRS. It is cheaper to reengineer functionality versus keeping a system that is primarily outdated" (DIMHRS 2008, 3). This method of "score carding," discussed earlier in this study, is a means of determining which systems get transferred to a new, interoperable system when full capability cannot be transferred from the legacy system.

As the DIMHRS website indicates, the program was initially started in 1995 and was the "cornerstone of transformation in the DoD" with the intent of bringing together over 80 legacy systems into the largest, worldwide human resources information system which handles over 3 million personnel and pay issues across the services (DIMHRS 2008, 2). At some point in the future, DIMHRS may be made available to interagency employees as well.

The JITC website offers the following rationale for DIMHRS inception and is important to the interoperability aspect of this study: "Lessons learned from Operation Desert Shield/Desert Storm emphasized problems in the DoD's ability to quickly mobilize a large task force composed of multiple components from the services.

Complicating mobilization efforts was the fact that each service has its own procedures for handling personnel and each is supported by unique (and aging) data systems. DIMHRS (Pers/Pay) is an initiative to provide a single point-of-entry system to collect, calculate, store, forward, and report personnel and pay data. DIMHRS (Pers/Pay) will support military personnel and pay offices worldwide and incorporate Active, Reserve, and National Guard personnel in garrison and deployed environments. Limited support is also provided for retired personnel, family members, and, during certain military operations, civilians and foreign nationals. DIMHRS (Pers/Pay) is the first stage of a larger defense reform initiative that will eventually support other DoD military Human Resources activities, such as manpower and training. The system will replace more than 80 legacy systems and support some 500+ external interfaces" (Joint Interoperability Test Command 2008, 1).

DIMHRS Implications

The largest implication of DIMHRS, once on-line, is that this will be the single largest personnel and pay resource application in the world simply because it will provide services to over three million employees. Given this fact and the fact that senior leaders will use this tool to address future operations, battles, and wars in pure terms of numbers, one can only presume that the enemy will view it similarly. DIMHRS may become not only a fully interoperable personnel and pay system, but also a large target for enemy exploitation in Cyberspace. The tradeoff for interoperable, joint systems that serve a large population, like the three million service members within DoD, is security.

DIMHRS security, like Defense Accounting and Finance Service security, will require multi-level security to keep personnel and pay data intact and free from attack.

Eliminating redundant, service-unique, legacy personnel and pay systems should improve information assurance under the DIMHRS umbrella. Although security creates a bigger target for the enemy to see and attack, it also creates centralized control, management, and execution across the services. As noted in the "Final Draft" of the DIMHRS Operational Requirements Document, June 1, 2004, Version 1.6 (Revised 12 July 2007), "Lack of Security. None of the Services' systems currently meets the DOD security standards. Government-wide requirements for information assurance and interoperability would be difficult and expensive to satisfy even if adequate numbers of technical personnel were available" (Department of Defense 2007, ES-3).

Another DIMHRS implication, also acknowledged in the Operational Requirements Document (ORD), is "DIMHRS (Pers/Pay) shall be designed to seamlessly integrate into the DoD environment. This includes compliance with existing and evolving standards as specified in the DoD IT Standards Registry, maximizing efficiency and performance in adverse environments, and integrating/interfacing with DoD and external systems. DIMHRS (Pers/Pay) shall also meet DoD security and information assurance guidelines and minimize the potential for unauthorized access to data. The DIMHRS (Pers/Pay) design must include the capability for rapid implementation of system changes to support requirements including legislative and policy changes" (Department of Defense 2007, 1-6). What this means from an interoperability standpoint is that the intent is to comply with the JTA and ultimately fit into the larger GIG as one would expect with any other C4I system. So in essence, DIMHRS is a joint program, managed by an appropriate level of management, and attempting to comply with existing interoperability guidance, discussed earlier in this study. "DIMHRS (Pers/Pay) will

provide joint interoperability spanning the functional areas of personnel and pay through an integrated environment in support of the warfighter and sustaining base" (Department of Defense 2007, 1-8). This is particularly important in a joint operating environment where the joint forces commander needs to know the status of his personnel spread throughout a theater. DIMHRS, as the joint, interoperable personnel and pay tool, will likely solve this dilemma as active duty, guard, and reserve personnel flow into and out of a joint operating area.

Another large DIMHRS implication is its ability to become JITC certified and accredited in accordance with the JCS/J6 validation process. DIMHRS data integrity and security must also be compliant with applicable service guidelines and DoDD policies. As indicated in the DIMHRS ORD, "the system must be certified and accredited in accordance with the DoD Information Assurance Certification and Accreditation Process (DIACAP). As part of this accreditation process, the EPMO [Enterprise Program Management Office] will coordinate with each Component to identify a Computer Network Defense service (CNDS) provider for the system as required under DODI O 8530.2" (Department of Defense 2007, 5-3) Not only does the program call for joint program management, funding, and responsibility, it also requires joint certification and accreditation with final approval at the JROC. This is currently the preferred method of seeking full interoperability for a joint C4I system.

DIMHRS Lingering Lessons

If there is one lingering lesson that clearly stands out as a difference between JTRS and DIMHRS program management, it is a lesson in fiscal levity. Levity in this sense means moving the control of program budgeting to a sufficiently high enough point

in an organization to effect real transformation and not just another stove pipe. In the case of DIMHRS, the DoD directed the services to jointly migrate toward an interoperable personnel and pay system. Both the Army and Air Force evaluated the PeopleSoft operating environment and agreed it would work for their purposes while the Navy opted to not comply and recommended another integrated solution called Marine Corps Total Force System (MCTFS) to better meet their needs (GAO-07-229 2006, 26). The GAO reported, "In 2005 we reported that DIMHRS . . . was not being managed as a DoD-wide investment, to include alignment with a DoD-wide architecture and governance by a DoD-wide body. In response, DoD has elevated the system to an enterprise investment under the Business Transformation Agency, and established a DIMHRS steering committee that is chartered to include representation from the services" (GAO-07-229 2006, 27). The Business Transformation Agency has also hired a DIMHRS program manager, and the Army and the Air Force, while continuing to evaluate their respective requirements, have determined that the commercial software product selected for DIMHRS can be used under certain conditions. The Army expects to deploy DIMHRS in 2008 and the Air Force plans to begin deployment in 2009.

The Navy, on the other hand, evaluated the capabilities of DIMHRS and MCTFS and determined that MCTFS would better meet its needs. According to a Navy official, "The Defense Business Systems Management Committee (DBSMC) directed the Navy to research MCTFS and to fully evaluate the cost implications of the MCTFS option, but has not granted the Navy permission to deploy MCTFS" (GAO-07-229 2006, 26). The Navy contends MCTFS is the best solution for sailors and marines to provide their personnel and pay support vice DIMHRS despite the DoD transformation efforts. Since

this was in stark contrast to the DoD spending thus far on DIMHRS of $668M, the GAO evaluated the Navy's progress to provide the Defense Business Systems Management Committee with a business case analysis on MCTFS/DIMHRS. The findings were filed in GAO 07-1139R, *Military Personnel: The Navy Has Not Provided Adequate Justification For Its Decision to Invest in MCTFS,* which was released on 26 July 2007. The GAO report cited the John Warner National Defense Authorization Act for Fiscal Year 2007, Public Law No. 109-364, §324 (2006) which directed the Secretary of the Navy to prepare a report about MCTFS focused on the following areas:

> A cost analysis of MCTFS alternatives to include a comparison between the costs of deploying and operating MCTFS within the Navy and the cost of including the Navy in DIMHRS.
>
> A business case analysis of the costs and benefits to both the Navy and DOD of the alternatives to MCTFS considered in the first objective.
>
> A compatibility analysis of MCTFS with the department's business enterprise architecture. (GAO-07-1139 2007, 1)

The Navy conducted the analyses indicated above and provided its findings to each task to the GAO in report 1139. Below are the Navy responses in summary:

> Either MCTFS or DIMHRS could provide basic personnel and pay capability for the Navy uniformed force at approximately equivalent cost.
>
> The DIMHRS alternative has substantially higher risks on cost, schedule, and function because MCTFS is already operational.
>
> MCTFS is fully compatible and compliant with the department's business enterprise architecture. (GAO-07-1139 2007, 2)

What the GAO discovered in the Navy response was a very superficial response lacking any depth as originally tasked by the Warner Act. The Navy did not comply nor complete the analyses originally tasked by the Warner Act on whether MCTFS or DIMHRS would best serve the DoD transformation efforts since they thought they had a

better solution in MCTFS. What the GAO report found was that the Navy simply answered the question with no regard to analysis and thus further stalled DIMHRS progress. So here is a joint, interoperable program that will replace over 80 legacy systems with one fairly compatible, low cost, commercial-off-the-shelf solution and the DoD cannot implement it throughout all services because of one service's stove pipe solution.

This raises many issues, previously discussed, that center around how the DoD implements, tracks, and executes C4I interoperability. If the Navy is able to stop integration of pay and personnel interoperability, then it seems logical that weapons systems integration will be even less likely to undergo the necessary interoperability and integration required to build the joint contemporary operating environment within the GIG. This is a DoD cultural challenge more so than a technical challenge, which is the focus of this study.

The cultural issue should be earmarked for other authors to research, discuss, and evaluate as possible delays in our venture to build a truly joint environment of C4I interoperable systems that span any service, nation, or coalition partner with lethal, accurate, and dependable data and information. This study notes the importance of cultural division between services but focuses on C4I interoperability challenges as related to process, programs, budget, acquisition, and command and control.

What did the GAO do after reviewing the Navy's cost benefit analysis, business case analysis, and compatibility analysis as originally chartered by Warner Act? The GAO, as in all ventures, provided the facts necessary to back up their claim that the Navy did not fully address the analysis requirements previously mentioned. Specifically, the

GAO found that the Navy did not "adequately justify" its decision to invest in MCTFS. Specifically the GAO cites:

> The Navy analysis of alternatives and the business case analysis of both MCTFS and DIMHRS were unreliable.
>
> The cost and benefit estimates used in these analyses were not sufficiently comprehensive, accurate, documented, or credible.
>
> The Navy's analysis shows that MCTFS is sufficiently compatible with DOD's business enterprise architecture [JTA] but the architecture lacks sufficient content to be used effectively to guide and constrain the acquisition of MCTFS. (GAO-07-1139R 2007, 3)

The complexity of C4I systems interoperability is evident in the case of the Navy's desire to field MCTFS as a replacement, or in lieu of DIMHRS; however, the bottom line up front is that the Warner Act "directed" DIMHRS implementation. Beyond technical complexity, as grounds for dismissing a joint solution to pay and personnel issues within the DoD, there seems to be a complacency or resistance to joint C4I solutions across the services. Given the GAO cited discrepancies above, it is important to look further into the reasons for the delays in DIMHRS implementation. A look at each cited discrepancy may help clear up the specific reasons for DIMHRS program delays.

First noted discrepancy in the GAO report was that the Navy's analysis of alternatives and its business case analysis were unreliable. If the Navy truly wanted to deploy MCTFS and the DoD provided it with an opportunity to prove MCTFS was the best solution, why would they provide unreliable analysis and alternatives, since this was their one opportunity to convince all of DoD that MCTFS was the right solution for everyone? The GAO found, through the course of the assessment and in conversations with high ranking Navy officials, like the Chief of Naval Operations, and DIMHRS PMs that the "Navy's analyses were unreliable because the cost and benefit estimates used for

these analyses were not sufficiently comprehensive, accurate, documented, or credible" (GAO-07-1139R 2007, 3).

In terms of alternatives, the Navy proposed implementing MCTFS service wide, DIMHRS service wide, or a combination of MCTFS initially followed by DIMHRS for all services after the Army and Air Force became fully functional. Clearly the costs for MCTFS and DIMHRS acquisition and deployment were readily available through their respective PM channels, but the third option of MCTFS followed by DIMHRS required some extensive research, which the GAO found the Navy just did not accomplish. Thus, the GAO found the Navy's alternative and cost benefit analysis data flawed since it was incomplete.

In its analysis, the Navy "excluded the third alternative, which was more costly than the MCTFS and DIMHRS alternatives. This exclusion skewed the results of the analyses by showing that the MCTFS alternative was the least costly solution" (GAO-07-1139R 2007, 4). This approach set the stage as MCTFS was cheapest, already working, and could satisfy two of the four services needs which in most cases would sell a program at the DoD level. Unfortunately for the Navy, the DoD already had invested $668 million into the DIMHRS program and there was great interest from onlookers during the course of this GAO report. The GAO also found that the Navy "cost estimates were not well-documented, because source data was not provided and the calculations performed for several cost elements were not explained" (GAO-07-1139R 2007, 5).

There were two significant, implied risks to the MCTFS/DIMHRS alternatives that the Navy proposed, which were not fully accounted for in their business case analysis. These risks were:

1. “The potential impact of moving MCTFS development operations from Kansas City to Indianapolis as part of the Base Realignment and Closure 2005 actions.” Navy MCTFS officials indicated they would delay closing the Kansas City site in order to mitigate impact to MCTFS fielding but there was no documentation to justify the expenses associated with this delay in the business case analysis provided by the Navy to the GAO. Nor could the Navy officials justify their authority to speak for their service in meeting the 2005 BRAC mandates to move MCTFS to Indianapolis (GAO-07-1139R 2007, 5).

2. “The potential impact of the contractor discontinuing its support of DIMHRS after 2013, as planned” (GAO-07-1139R, 2007, 5). After the Navy’s report, the DIMHRS contractor said it would support DIMHRS indefinitely, but this support would be limited. “For example, ‘sustaining support’ does not include key services, such as new updates, product fixes, security alerts, critical patch and regulatory updates, and certification of DIMHRS with new products developed by the contractor. It is unclear what the costs, if any, will be for this sustaining support” (GAO-07-1139R 2007, 4). The GAO concluded that even though the contractor decided to extend DIMHRS support beyond 2013, this did not constitute a binding legal agreement, and the contractor could just as easily decide to discontinue its support of DIMHRS or increase DIMHRS support costs. Given the lack of accuracy of these cost estimates, the GAO found they could not rely on any of the benefits or cost savings reported by the Navy. This earned the Navy the title on the GAO report, *The Navy Has Not Provided Adequate Justification For Its Decision to Invest in MCTFS*, and put MCTFS and DIMHRS integration at a standstill.

The GAO also made this connection in their 2006 report in which it described this chasm between current force structure and a truly joint force: The "major reason the department has thousands of business systems is that it has historically failed to consistently employ the range of effective institutional investment management controls, such as an architecture-centric approach to investment decision making, that our work and research show are keys to successful system modernization programs. Such controls help to identify and eliminate duplicative systems and this helps to optimize mission performance, accountability, and transformation. They also help to ensure that promised system capabilities and benefits are delivered on time and within budget" (GAO-07-229 2006, 24). The architecture-centric approach could be construed as following the JTA while the controls for joint implementation of systems would be the certification and validation by JITC and JCS/J6. This is the case with JTRS as well and for that matter any C4I system in the future using any one of a number of incremental acquisition models.

DIMHRS is a good example of a program the DoD needs now, or has needed since its inception in 1995; yet it is at step one of a three-phase implementation plan after eight years of development. Some of the delays may be attributed to changes in policy, doctrine, technology, acquisition, or budget, but the same dilemma surfaced in DIMHRS that did in JTRS--unknown requirements and lack of definitive direction by all services. The unknown requirements were a direct result of an unknown common operating environment, architecture, and GIG. The unknown direction is a result of service unique solutions to a DoD-wide interoperable system like DIMHRS or JTRS. This is exacerbated by the fact that not one entity or organization is effectively designing,

managing, delivering, and funding the GIG. Its development hinges upon service-unique systems, independently funded and directed by a service, and stands as one of the most significant roadblocks to full C4I interoperability.

The DIMHRS and JTRS programs typify examples of institutional impediments to DoD's transformation efforts to create truly joint interoperability among the services, allies, and coalition partners. The DIMHRS and JTRS programs morphed so many times to take on a new face over the years that the transformation effort actually slowed down the acquisition and fielding process, to a standstill in the case of DIMHRS, and continues to even after decades of oversight and management at very high levels within the DoD. DIMHRS, as opposed to JTRS, is a smaller program centered on DoD personnel and pay systems and should have been easier to implement in the grander picture of C4I interoperability, but is not being implemented as a joint program due to the Navy's insistence there is a better solution in MCTFS. It was not until November 2007, that the DoD finally convinced the Navy to get on board with DIMHRS, and now it will be fielded as a joint solution, some eight years after inception.

CHAPTER 5
CONCLUSIONS AND RECOMMENDATIONS

Introduction

This study examined C4I systems interoperability in the DoD and focused on existing law, strategy, as provided by the National Command Authorities down to each service, and methods of certification and accreditation. Looking through the *NMS*, *NDS*, Goldwater-Nichols Act of 1986, and a variety of Joint Staff and DoD instructions and directives down to the program management level provided a base to compare and contrast interoperability progress. The largest gear in the interoperability machine is clearly acquisition and much time was devoted to evaluating how service budgets decide what is and is not funded from an interoperability standpoint. Once the guidance for C4I was established, an in-depth review of two ongoing joint programs within the DoD, namely JTRS and DIMHRS, provided some insight into interoperability challenges in real time. This study also focused on the positive changes to law, strategy, doctrine, guidance, certification, and validation and determined much progress has taken place since the year 2000, although there is much room for improvement as well.

C4I interoperability is a complex capability to plan, acquire, fund, and prove in an organization as large as the DoD and amongst allies and coalition partners. Through the course of this study, it is apparent that volumes of directives, joint architecture and standards, acquisition rules, and strategic infrastructure concerns were fielded since Black's thesis in 2000. Most notably was the development of the JTA used to ensure C4I interoperability through common data standards and interfaces. The JTA, as a source document, provides solid ground from which a current program can be designed and implemented and ultimately become an integral part of the GIG, which drives the concept

of netcentricity. In this regard, the JTA is a substantial development, which should help improve C4I interoperability across service lines and country borders.

Secondary Research Questions

Secondary Research Question: "What life cycle planning tools exist to ensure C4I interoperability success within the DoD and joint environment?"

Clearly, since 2000, the U.S. made dramatic improvements in the ways and means it plans, develops, acquires, and fields C4I systems as found in the JTRS and DIMHRS case studies in chapter 4. A great deal of time was spent researching and documenting the JCS/J6 validation process in chapter 2 which provides the oversight of all C4I systems that pass through the JITC certification system. JITC has the means of "checking out" virtually any C4I system. In the case of JTRS, it built an entire test facility devoted to JTRS certification and evaluation and the JTRS JPEO absorbed the costs associated with it.

In a report, *Steps Needed to Ensure Interoperability of Systems That Process Intelligence Data* in 2003, the GAO report recommended "that DoD take steps needed to enforce its certification process and determine why the services are slow to certify their systems in order that it can implement the controls and incentives needed to spur compliance" (GAO-03-329 2003, 5). The DoD generally agreed with the GAO report findings but once again pointed toward the JCS/J6 oversight process as the necessary tool to ensure interoperability requirements were fully realized in close coordination with JITC. As demonstrated within this study, the JCS/J6 process, although comprehensive and synchronized with JITC efforts, lacks the budgetary controls and muscle to incentivize the certification process within DoD.

Even after the publication of the JTA, CJCSIs, DoDDs, and QDRR firmly suggested and required joint interoperability in newly fielded systems, the GAO found that "only 2 of 26 Distributed Common Ground-Surface System (DCGS) systems have been certified as interoperable, because 21 of the systems that have not been certified have already been fielded" (GAO-03-329 2003, 2). The DCGS system was initiated in 1998 and planned as a "migration to an overarching, interconnected family of systems for processing intelligence data" used across DoD, much like JTRS was when conceived in 1997 for radios (GAO-03-329 2003, 2). If the goal of DCGS was interoperability, how could 21 of the 26 subsystems escape the certification and validation processes? As in the JTRS case study, this was not a program mired in ever changing requirements and scope, nor as in the case of DIMHRS was it caught in an endless loop of one service looking for "another" solution that "might" meet DoD needs. Why then did a program from 1998, with the intent of fielding an interoperable family of intelligence systems, avoid interoperability testing on such a grand scale?

The GAO pointed out that in 1998 the DoD began its watchdog list of interoperability programs not meeting standards to provide another layer of oversight, yet even in 2003 the following discrepancies existed:

> DoD's process for testing and certifying that ground-surface based processing systems will be interoperable is not working effectively. Because 21 of the systems that have not been certified have already been fielded, there is greater risk that the systems cannot share data as quickly as needed. Moreover, while certifications are planned for 17 of the 26 systems, they are not planned for 7 others.
>
> System managers are more focused on getting systems fielded quickly and/or they do not want to fund the certification process, as DoD requires them to do. Our work has also shown that the military services focus more on meeting their own requirements when developing new systems as opposed to requirements that would facilitate operating jointly with other services.

> One reason why the process is not working effectively is the incomplete planning discussed above, including the lack of an overarching test plan. (GAO-03-329 2003, 5)

The DCGS report furthers the idea that the DoD has the means to certify and accredit joint interoperable C4I systems but for a variety of reasons does not.

Faughn summarized seven reasons DoD does not complete the JCS/J6 and JITC interoperability processes discussed earlier. These reasons included: "The military acquisition culture, dwindling budgets, rapidly changing technology, the changing nature of operations, competing priorities, insufficient oversight, and unrealistic training and exercises" (Faughn 2002, 31). As Faughn noted, and this study confirmed, the services employ an acquisition strategy that many times stove pipes C4I systems unique to that service. Although this may have been out of necessity in the past due in large part to the lack of jointness, the U.S. is in the midst of ever changing technology, which drives an even greater need for interoperability. "Dwindling budgets" are more a product of rising software development costs than shrinking military spending, and make the interoperability bills harder to pay. Although certification costs are miniscule compared to total system cost, PMs continually wrestle with money that could otherwise fund additional capabilities vice certification and validation. "The cost to certify the Army's $95 million Common Ground Station, for example, was $388,000" (GAO-03-329 2003, 13). Insufficient oversight, also noted by Faughn as a contributing factor to the lack of interoperability testing within the DoD, remains a primary driver in today's C4I environment as discussed in the JTRS and DIMHRS case studies. Watchdog lists or organizations cannot fix this problem for DoD. As this study recommends, one agency or organization needs to be appointed to control the money and processes that will ensure

DoD has a suite of lethal C4I systems to carry out missions directed by the National Command Authorities.

Secondary Research Question: "Is C4I interoperability a plausible schema for future joint and coalition operations?"

Yes, it is not only plausible but also absolutely necessary. While time, cost, and performance continue to challenge program managers seeking to field C4I systems quickly, under budget, and within tolerances, interoperability requirements must be addressed with equal vigor within those cycles. With the tools available today within the DoD and support from the federal law, National Command Authorities, services, allies, and coalition members, the C4I community can migrate operations to one common GIG and create a truly joint, interoperable environment capable of precise, coordinated, and lethal effects anywhere on the globe.

Research Question

Primary Research Question: "What do U.S. military services need to achieve C4I interoperability in an effort to streamline operations?"

The U.S. military services need help in order to achieve the means to plan, develop, and acquire new C4I systems that are truly interoperable with other services, allies, and coalition members. The Goldwater-Nichols Act of 1986 requires "jointness" but lacks any depth in terms of C4I interoperability requirements. New legislation aimed at laying out a DoD wide strategy for the life cycle management of C4I systems across the air, land, sea, space, and cyberspace domains would begin the formality that is lacking in current day interoperability processes. *NDS* and *NMS* both support, in detail, the idea of joint, interoperable C4I systems so little change is required to these strategic

documents. The CJCSI series and DoDD series are quite comprehensive and appear adequate to ensure C4I compliance with the JTA. Beyond this is where guidance successes since 2000 become blemished by organizational voids.

Service responsibilities for the procurement and deployment of Joint Staff directed capabilities through the JCIDS process flow successfully but often skip interoperability checks and balances. Stove piped C4I systems continue to be fielded to satisfy service requirements and JCIDS capabilities many times contrary to interoperability standards defined above, as in the case study of DIMHRS. The Joint Staff directs the services to develop certain capabilities through the JCIDS process, but it has no recourse when services either fail or disregard those directions. Since the money is controlled by the respective service, there are few incentives to comply with interoperability certification and validation requirements. The JCS/J6 oversees all such efforts and checks up on C4I systems that are entered into the certification and validation cycle conducted through the JITC, but it has little means of determining what systems may be underway within each service, which may also require interoperability testing and evaluation. Acquisition processes incorporated changes to keep pace with technology since 2000, but they are not directly tied to C4I interoperability checks and balances discussed in this study.

The FCS acquisition strategy, employed by the Army, uses the "Spin Out" concept to deliver new C4I tools to Soldiers, Sailors, Airmen, and Marines in the field more quickly than conventional incremental acquisition processes of the past. FCS will become an integral part of the GIG in the future and will receive its wireless network services through a variety of other GIG compliant programs like JTRS. As the DoD

plans, develops, funds, and deploys C4I systems today, it must also determine the interoperability required to operate within the GIG in the future, or there may be consequences derived from an inability to communicate or to put a bomb on target in the fluidity of battle.

This study demonstrated that the DoD has the means, processes, and written guidance at its disposal to ensure interoperability one system at a time. This study also demonstrated that within DoD no one person, agency, or organization has oversight and fiscal authority of interoperability over any service, which fails to comply with established policies. In order for the U.S. to move forward and provide an efficient means of ensuring C4I interoperability across the services, with allies, and among the coalition partners, there must be centralized control of the interoperability budget, program management, certification and validation, testing and evaluation, fielding, and life cycle management. As Faughn discovered, during his 2002 Fellowship in a study on interoperability, "Ultimately, no one is in charge of the process. Although this situation may have come about by design and for good reason . . . to thwart any overzealous person or organization . . . it has led to a culture or environment with a significant, and unfortunate, impact on efforts to achieve interoperability" (Faughn 2002, 31).

Even after the *QDRR* of 2006 identified the DoD roadmap for future operations by pinpointing the importance of C4I interoperability, the U.S. failed to attain its desired level of joint capability. Much has been written, including Black's thesis on interoperability, Faughn's study, and many other reports which research whether we "are there yet," but what seems to be missing is the recommended solution sets to fix the DoD interoperability discrepancies. It is safe to assume that C4I interoperability will continue

to be a high priority within the DoD for the foreseeable future as it is identified in not only law, but also doctrine, strategy, and practice from the *NMS* down to service unique instructions, so this leg of the process is intact. As this study discovered, a great deal of concentrated work went into establishing the JTA, DoDDs, CJCSIs, and similar service policies that support the migration of all platforms and systems onto the GIG.

The other leg, which is not intact, identified a lack of a central authority and organization with the responsibility of exacting the established interoperability standards and cross checking future DoD investments to eliminate duplication in dollars and effort. One could argue the DoD CIO or the JCS/J6 has this authority, but what they both lack is fiscal control, since neither has the budget to fix known C4I interoperability shortfalls. Shrinking budgets and risings costs of software development require more than oversight at the Joint Staff level. In an era where the DoD expects to spend $200 billion on C2 software development within the next decade, this is an easy sell (NAVSEA 2005, 3).

So how does the U.S. get a firm grip on the entire C4I interoperability process and move the nation forward and in synch with its allies and coalition members. Following are four recommendations, by the author, to achieve the control necessary to implement full C4I interoperability within the DoD:

1. Tie all service-related budgeting to the JCIDS process and give an agency or organization the power to control and influence military and commercial vendors to complete C4I interoperability priorities for the DoD.

2. Rewrite the Goldwater-Nichols Act of 1986 so it accurately reflects the joint requirements of DoD C4I interoperability placing emphasis on the agency and or organization identified in number one.

3. Rewrite *NDS* and *NMS* to identify and layout strategy for future operations, battles, and wars, which require use of the GIG and the C4I interoperability components, which comprise it. Levy management responsibility to agency and or organization identified in number one.

4. Combine the JCS/J6 validation and the JITC certification processes into one cohesive system, managed by one agency (identified in number one), and tied to the DoD Acquisition System so new facilities, equipment, weapons, and systems are planned, developed, and implemented as fully C4I interoperable. Any system attached to the GIG must pass through these interoperability checks and balances.

Recommendations for Further Study

Several areas were uncovered which would help further the effort of one day reaching full C4I interoperability within the DoD and potentially with U.S. allies and coalition members. This thesis did not incorporate these areas into the research:

1. How does the acquisition community view the need and desire of the DoD to attain C4I interoperability when completing the Planning, Programming, Budgeting, and Execution cycles? In that regard, do the acquisition rules of the road allow for centralized control of funds with the goal of ultimately saving money, but simultaneous to that, deploying the required capabilities identified by the JCS as "must haves" for war?

2. Is there another method or system for completing interoperability testing, certification, and accreditation that exists in industry or elsewhere in the world which might simplify the process of building C4ISR systems of the future to "automatically" interoperate using global interfaces identified within the JTA or some other common architecture and standards?

3. Is C4I interoperability testing and certification worth the effort in an organization as large as the DoD and with the variety of missions, some of which are service specific, that must be carried out anywhere on the globe? Should the entire idea of interoperability be dismissed as “too hard” and “too expensive” which thus allows for and encourages “stovepipes”?

4. If a rewrite of the Goldwater-Nichols Act became a reality, what other current day changes, besides C4I interoperability, should be made to bring it in line with ongoing operations and budget realities of the future.

REFERENCES

Black, Michael B. 2000 “Coalition command, control, communications, computer, and intelligence systems interoperability: A necessity or wishful thinking?” Thesis, Command and General Staff College, Fort Leavenworth, Kansas.

Bunker, Robert J. 2003. *Non-state threats and future wars.* New York, NY: Frank Cass and Co.

Chairman, Joint Chiefs of Staff. 2004. *The national military strategy of the United States of America: A strategy for today; a vision for tomorrow*. Washington, DC: Government Printing Office.

———. 2006. Command, Control, Communications and Computer Systems Directorate J6. *Joint net-centric operations campaign plan*. Washington, DC: Government Printing Office.

Commandant of Marine Corps. 1989. Marine Corps Order 3093.1C, *Intraoperability and interoperability of marine corps tactical C4I systems.* Washington, DC: Government Printing Office. http://www.usmc.mil/directiv.nsf/73dd6bb050e72cf385256bca0072322f/c9a2bbb5d482ed9685256497005ae237/$FILE/MCO%2030 93.1C.pdf (accessed 23 September 2007).

Defense Information Systems Agency (DISA). 2007. “Joint interoperability support.” http://www.disa.mil/main/about/jointis.html (accessed 23 September 2007).

Defense Integrated Military Human Resource System (DIMHRS). 2008. Homepage. http://www.dimhrs.mil/background.html (accessed 23 April 2008).

Department of the Army. “Future combat system (FCS) program overview: FCS 101.” https://www.fcs.army.mil/program/index.html (accessed 8 April 2008).

Department of Defense. 2003. *Joint technical architecture (JTA), vol. 1*. Washington, DC: Government Printing Office. http://www.acq.osd.mil/osjtf/pdf/jta-vol-I.pdf (accessed 23 September 2007).

———. 2005a. Department of Defense Directive (DoDD) 5144.1, *Assistant secretary of defense for networks and information integration DoD chief information officer (ASD(NII)/DoD CIO)*. Washington, DC: Government Printing Office.

———. 2005b. *The national defense strategy of the United States of America.* Washington, DC: Government Printing Office.

———. 2006. *Quadrennial defense review report.* Washington, DC: Government Printing Office.

_____. 2007. *Defense integrated military human resources system (DIMHRS), (personnel and pay), operational requirements document,* 1 June 2004, Version 1.6 (Revised 12 July). https://www.mpm.osd.mil/documents/DIMHRS_ORD_ MilestoneC08.pdf (accessed 28 April 2008).

Director of Command, Control, Communications, and Computers (C4) Systems (J-6), The Joint Staff. *Synchronize network delivery joint interoperability test certification: "Foundation of net centric operations & future joint warfighting."* http://www.jcs.mil/j6/c4campaignplan/interoperability_supportability_fact_sheet. pdf (accessed 2 February 2006).

Faughn, Anthony W. 2002. *Interoperability: Is It Achievable?* Cambridge, MA: Center for Information Policy Research, Harvard University. http://www.gao.gov/ new.items/d02100r.pdf (accessed 23 April 2008).

General Accounting Office. 1998. GAO-98-073, *Joint military operations: Weaknesses in DOD's process for certifying C4I systems' interoperability.* Washington, DC: Government Printing Office. http://www.fas.org/irp/gao/ nsiad98073.htm (accessed 23 September 2007).

———. 2003a. GAO-03-329, *Defense acquisitions: Steps needed to ensure interoperability of systems that process intelligence data.* Washington, DC: Government Printing Office. http://www.gao.gov/new.items/d03329.pdf (accessed 2 May 2008).

———. 2003b. GAO-03-879R, *Challenges and Risks Associated with the Joint Tactical Radio System Program.* http://www.gao.gov/htext/d03879r.html (accessed 6 April 2008).

———. 2003c. GAO-03-829, *Technology Transfer: NIH-Private Sector Partnership in the Development of Taxol.* Washington, DC: Government Printing Office. http://www.gao.gov/htext/d03829.html (accessed 28 October 2007).

———. 2005. GAO-05-189, *DOD Systems Modernization, Management Of Integrated Military Human Capital Program Needs Additional Improvements.* http://www.gao.gov.htext/d05189.html (accessed 2 April 2008).

Government Accountability Office. 2006a. GAO-06-955, Defense Acquisitions: Restructured JTRS Program Reduces Risk, but Significant Challenges Remain. Washington, DC: Government Printing Office. http://www.gao.gov/new.items/ d06955.pdf (accessed 28 October 2007).

———. 2006b. GAO-07-229, *A Comprehensive Plan, Integrated Efforts, and Sustained Leadership Are Needed to Assure Success*. Washington, DC: Government Printing Office. http://www.gao.gov/new.items/d07229t.pdf (accessed 28 April 2008).

———. 2007a. GAO-07-388, *An integrated portfolio management approach to weapon system investments could improve DOD's acquisition outcomes.* Washington, DC: Government Printing Office. http://www.gao.gov/new.items/d07388.pdf (accessed 21 April 2008).

———. 2007b. GAO-07-1139R, *Military personnel: The navy has not provided adequate justification for its decision to invest in MCTFS.* Washington, DC: Government Printing Office. http://www.gao.gov/new.items/d071139r.pdf (accessed 29 April 2008).

Gause, Kenneth, Catherine Lea, Daniel Whiteneck, and Eric Thompson. *U.S. Navy interoperability with its high-end allies*. Alexandria, VA: Center for Strategic Studies. http://www.DoDccrp.org/events/5th_ICCRTS/papers/Track3/080.pdf (accessed 23 September 2007).

Hamilton, John A., Lt Col, Captain Jerome D. Rosen, USAF, and Major Paul A. Summers, USAF. "An interoperability road map For C4ISR legacy systems." *Acquisition Review Quarterly* (Winter 2002): 17-32. http://www.dau.mil/pubs/arq/2002arq/Hamilton.pdf (accessed 23 September 2007).

House Armed Services Committee. 2003a. Statement By Lieutenant General William S. Wallace, Commanding General, Combined Arms Center, U.S. Army Training And Doctrine Command Before The Subcommittee On Terrorism, Unconventional Threats And Capabilities Armed Services Committee United States House Of Representatives On C4I Interoperability: New Challenges In 21st Century Warfare. 21 October 2003. http://www.globalsecurity.org/military/library/congress/2003_hr/03-10-21wallace.htm (accessed 23 September 2007).

_____. 2003b. *Terrorism, unconventional threats and capabilities Subcommittee will meet to receive testimony on C4I Interoperability: New challenges in 21st century warfare*. Opening comments by Rep. Jim Saxton. 21 October 2003. http://www.iwar.org.uk/rma/resources/c4i-interoperability/index.htm (accessed 23 September 2007).

_____. 2007. *Statement of Admiral William J. Fallon on the Posture of USCENTCOM, 21 March 2007.* In "C205: Department of Defense Organization and Process, Reading E." Fort Leavenworth, KS: US Army Command and General Staff College, June 2007.Joint Chiefs of Staff. 2006. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01D, *Interoperability and supportability of information technology and national security systems.* Washington, DC: Government Printing Office.

Joint Expeditionary Force Experiment (JEFX). 2007. https://jefxlink.langley.af.mil.index.asp (accessed 28 May 2008).

Joint Interoperability Test Command (JITC). 2007. "*Global command and control system (GCCS), interoperability (IOP).* Home page. http://jitc.fhu.disa.mil/ gccsiop/ (accessed 23 September 2007).

Joint Interoperability Test Command (JITC). 2008. Projects Link. http://jitc.fhu.disa. mil/washops/jtcb/dimhrs.html (accessed 28 April 2008).

Joint Program Executive Office (JPEO) for Joint Tactical Radio System (JTRS). 2006. "Organizational overview." http://enterprise.spawar.navy.mil/body. cfm?type=c& category=27&subcat=60 (accessed 6 April 2008).

_____. 2008. "Connecting the tactical edge." http://jpeojtrs.mil/files/org_info/ JTRS_Fact_Sheet.pdf (accessed 8 April 2008).

Kanewske, Paul. 2002. "Joint C4I interoperability: A long history, a tenuous future." Research Project, Naval War College, Newport, RI. http://www.stormingmedia. us/55/5519/A551904.html (accessed 23 September 2007).

Kasunic, Mark, and William Anderson. 2004. *Measuring systems interoperability: Challenges and opportunities*. http://www.sei.cmu.edu/pub/documents/ 04.reports/pdf/04tn003.pdf (accessed 23 September 2007).

Koziol, Craig, Major General. 2007. "New focus on U. S. Air Force ISR." *C4ISR, The Journal of Net Centric Warfare* (3 September). http://www.c4isrjournal.com/ story.php?F=2892613 (accessed 23 September 2007).

Martinage, Robert. 2007. "Technological implications of the 2006 quadrennial defense review." The Center for Strategic and Budgetary Assessments (CSBA) Online, Power Point Presentation. http://www.csbaonline.org/4Publications/PubLibrary/ S.20070221.Technological_Impl/S.20070221.Technological_Impl.pdf (accessed 28 October 2007).

National Academy of Science. 1999. *Realizing the potential of C4I.* Washington, DC: National Academy Press. http://books.nap.edu/html/C4I/notice.html (accessed 23 September 2007).

Naval Sea (NAVSEA) Warfare Center. 2005. *Military communications strategic insight.* Crane, IN: Government Printing Office.

Saxton, Jim, Representative. 2003. "C4I interoperability to our warfighter." *Military Information Technology Online* 11, no. 7. http://www.military-information-technology.com/article.cfm?DocID=348 (accessed 23 September 2007).

INITIAL DISTRIBUTION LIST

Combined Arms Research Library
U.S. Army Command and General Staff College
250 Gibson Ave.
Fort Leavenworth, KS 66027-2314

Defense Technical Information Center/OCA
8725 John J. Kingman Rd., Suite 944
Fort Belvoir, VA 22060-6218

Lt Col John B. Esch
DIJMO
USACGSC
100 Stimson
Fort Leavenworth, KS 66027-1352

Dr. Alexander M. Bielakowski
DMH
USACGSC
100 Stimson
Fort Leavenworth, KS 66027-1352

Lt Col J. D. Rye
AFELM
USACGSC
100 Stimson
Fort Leavenworth, KS 66027-1352